Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Рекомендації щодо оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Анна ТОРЧИЛО**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Торчило Анні Петрівні**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Рекомендації щодо оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція хмарних обчислень, загрози хмарних технологій, нормативно-правова база у сфері захисту інформації, методи забезпечення інформаційної безпеки хмарних систем

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомлення з теорією хмарних технологій, їх різновидами та вразливостями, розгляд стандартів з інформаційної безпеки технологій хмарних обчислень, розробка переліку вимог для оцінювання відповідності надавачів хмарних послуг умовам інформаційної безпеки

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Анна ТОРЧИЛО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Постановка задачі, оформлення завдань	29.10.2021 – 20.01.2022	*виконано*
2	Аналіз наукової літератури	21.01.2022 – 10.02.2022	*виконано*
3	Аналіз нормативно-правової бази	11.02.2022 – 16.02.2022	*виконано*
4	Дослідження концепції хмарних обчислень	17.02.2022 – 03.03.2022	*виконано*
5	Аналіз загроз інформаційної безпеки в технологіях хмарних обчислень	04.03.2022 – 21.03.2022	*виконано*
6	Розробка процесу оцінювання відповідності вимогам.	22.03.2022 – 01.04.2022	*виконано*
7	Формування вимог до інформаційної безпеки надавачів хмарних послуг.	02.04.2022 – 11.05.2022	*виконано*
8	Оформлення пояснювальної записки	12.05.2022 – 26.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	27.05.2022 – 13.06.2022	*виконано*

Завдання видав _____ Сергій ДАКОВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Анна ТОРЧИЛО
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка: дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 84 сторінку та 13 рисунків. Список використаних джерел, має обсяг 4 сторінки, і складається з 36 найменувань. Крім того, робота містить 8 додатків із загальною кількістю сторінок 44.

Об'єктом дослідження є процес оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг.

Метою роботи є підвищення безпеки та правомірності використання технологій хмарних обчислень шляхом розробки рекомендацій з проведення процедури оцінювання відповідності та вдосконалення переліку вимог до інформаційної безпеки надавачів хмарних послуг.

Предметом дослідження є модель оцінювання надавачів хмарних послуг щодо відповідності вимогам інформаційної безпеки.

Методи дослідження використанні при підготовці дипломної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів та нормативно-правової бази України;
- узагальнення державної та міжнародної практики.
- порівняння та синтез.

В роботі проведено дослідження основних понять технологій хмарних обчислень, розглянуто їх різновиди та особливості функціонування.

Проаналізовано загрози інформаційної безпеки хмарних сервісів.

Розглянуто основоположні стандарти та нормативно-правову базу України, які регулюють питання інформаційної безпеки хмарних сервісів.

Розроблено схему вимог для оцінювання інформаційної безпеки надавачів хмарних послуг.

Практична цінність отриманих результатів полягає в розробці рекомендацій щодо оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг.

Напрямки подальших досліджень: розробка автоматизованої комплексної схеми для сертифікації надавачів хмарних послуг щодо відповідності вимогам інформаційної безпеки.

Ключові слова: технології хмарних обчислень, хмарні послуги, хмарний сервіс, моделі розгортання, загрози, вимоги до інформаційної безпеки, стандартизація, процедура оцінювання відповідності, кібербезпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

API	–	Application programming interface
BIA		Business Impact Analysis
BYOD		Bring your own device
CCM		Cloud Control Matrix
CRM	–	Customer relationship management
CSA	–	Cloud Security Alliance
CSA		Cloud Security Alliance
CSF	-	Cybersecurity Framework
CSP-CERT		Cloud Service Provider Certification
CVSS		Common Vulnerability Scoring System
DDoS	–	Distributed denial-of-service
DLP	–	Data Loss Prevention
ERM		Enterprise Risk Management
ERP	–	Enterprise resource planning
EUCS		European Cybersecurity Certification Scheme
FedRAMP		The Federal Risk and Authorization Management Program
FISMA		Federal Information Security Modernization Act
GDPR		General Data Protection Regulation
HIPAA		Health Insurance Portability and Accountability Act
IaaS	–	Infrastructure-as-a-Service
IAM	–	Identity and Access Management
IEC		International Electrotechnical Commission
ISO	–	International Organization for Standardization
NIST	–	National Institute of Standards and Technology
PaaS	–	Platform-as-a-Service
PCI-DSS	–	Payment Card Industry Data Security Standard
RACI		Responsibility Assignment Matrix
RPO		Recovery Point Objective
RTO		Recovery Time Objective
SaaS	–	Software-as-a-Service
SIEM		Security information and event management

SLA	–	Service Level Agreement
SOC		Service Organization Control
SSO		Single sign-on
SSRM		Shared Responsibility Model in the Cloud
STAR		Security, Trust, Assurance and Risk
TVM		Threat and Vulnerability Management
ВМ		Віртуальна машина
ДСТУ		Державний стандарт України
ЄС		Європейський союз
ІзОД		Інформація з обмеженим доступом
КСЗІ	–	Комплексна система захисту інформації
НХП	-	Надавач хмарних послуг
ОЗ		Обліковий запис
ОС		Операційна система
ПЗ	–	Програмне забезпечення
ПІБ		Політика інформаційної безпеки
СУІБ	–	Система управління інформаційною безпекою
ЦОД	–	Центр обробки даних
ШПЗ	-	Шкідливе програмне забезпечення

ЗМІСТ

ВСТУП

Актуальність. Технології хмарних обчислень залишаються глобальним трендом впродовж останніх років завдяки безлічі переваг порівняно з традиційними інформаційно-телекомунікаційними системами. Проте вони не можуть нівелювати проблеми інформаційної безпеки, яку приховують в собі хмарні послуги. Більше того, особливості багаторівневої хмарної інфраструктури збільшують плацдарм для можливостей зловмисників і помилок працівників. Саме тому, перед міграцією до хмари потенційні користувачі повинні комплексно оцінити рівень гарантій безпеки на всіх рівнях хмарної інфраструктури, беручи до уваги відповідність надавачів хмарних послуг визнаним галузевим і національним стандартам інформаційної безпеки.

Оскільки нормативно-правова база України, яка стосується хмарних послуг наразі перебуває процесі трансформації, проблема визначення процедури оцінювання відповідності та формулювання схеми вимог, яку можна використати для підтвердження необхідного рівня інформаційної безпеки надавачів хмарних послуг залишається актуальною.

Тому **метою роботи** є підвищення безпеки та правомірності використання технологій хмарних обчислень шляхом розробки рекомендацій з проведення процедури оцінювання відповідності та вдосконалення переліку вимог до інформаційної безпеки надавачів хмарних послуг.

Для досягнення визначеної мети необхідно вирішити наступні **завдання:**

- дослідити основні поняття технологій хмарних обчислень, їх різновиди та особливості функціонування;
- проаналізувати загрози інформаційній безпеці, притаманні хмарним сервісам;
- розглянути основоположні стандарти та законодавчу базу України, які регулюють питання інформаційної безпеки хмарних сервісів;

- розробити схему вимог для оцінювання інформаційної безпеки надавачів хмарних послуг.

Об'єктом дослідження в даній роботі є процес оцінювання відповідності вимогам інформаційної безпеки для надавачів хмарних послуг.

Предметом дослідження в даній роботі є модель оцінювання надавачів хмарних послуг щодо відповідності вимогам інформаційної безпеки.

Методи дослідження використанні при підготовці дипломної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів та нормативно-правової бази України;
- узагальнення державної та міжнародної практики.
- порівняння та синтез.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ХМАРНИХ ТЕХНОЛОГІЙ

1.1 Основні поняття хмарних обчислень

Ринок хмарних інформаційних технологій інтенсивно розвивається – відповідно до результатів досліджень Gartner, у 2022 році витрати кінцевих користувачів на публічні хмарні рішення зростуть до 494,7 мільярдів доларів на 20,4% більше порівняно з 410,9 мільярдів доларів у 2021 році, а в 2023 очікується, що ринок хмар сягне майже 600 мільярдів доларів [1]. Незважаючи на таку популярність хмарних послуг, певною мірою зберігається термінологічна лакуна у цій галузі, що може викликати незручності в експертних оцінках та правовій практиці.

Згідно з визначення, що надає Національний інститут стандартів і технологій (далі - NIST), хмарні обчислення – це «модель, що забезпечує постійний зручний доступ за вимогою до спільної мережі змінюваних обчислювальних ресурсів, які можуть швидко надаватись для використання з мінімальними адміністративними витратами або втручанням з боку надавача хмарних послуг» [2]. Така дефініція достатньо повно розкриває суть явища, проте українське законодавство схиляється до формулювання від Міжнародної організації зі стандартизації (далі - ISO), що визначає хмарні обчислення як «парадигму для сприятливого мережевого доступу до масштабованого еластичного пулу фізичних або віртуальних ресурсів, які можна спільно використовувати із самообслуговуванням і адмініструванням за вимогою» [3]. Таким чином, хмарні технології можна розглядати як сукупність хмарних сховищ і хмарних обчислень як технології обробки даних в цих сховищах, а хмарні послуги – як послуги з надання хмарних ресурсів за допомогою технології хмарних обчислень (відповідно до Закону України «Про хмарні послуги») [4].

Як результат, з’являється потреба у формулюванні поняття хмарних ресурсів. Ними вважаються будь-які компоненти інформаційної системи, доступ до яких забезпечують технології хмарних обчислень [5].

Закон України також передбачає визначення учасників відносин у сфері хмарних обчислень – користувач, який використовує хмарні послуги та надавач, який ці послуги надає (далі - НХП).

На високому рівні, як хмарні, так і традиційні технологій обчислень дотримуються логічної моделі, що представлена на рис. 1, яка допомагає ідентифікувати різні рівні на основі функціональності та наочно демонструє відмінності між різними моделями обчислень.

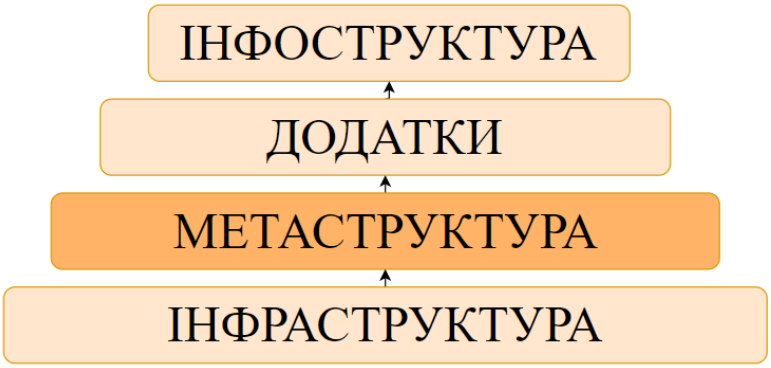

Рисунок 1 - Логічна модель хмарних обчислень

Інфраструктура: основні компоненти обчислювальної системи: процесор, мережа та сховище. Їх можна назвати фундаментом, на якому будується все інше.

Метаструктура: протоколи та механізми, які забезпечують інтерфейс між рівнем інфраструктури та іншими рівнями. Цей рівень пов’язує технології та забезпечує управління та налаштування системи.

Структура додатків: програми, розгорнуті в хмарі, і базові служби додатків, які використовуються для їх створення.

Інфоструктура: Дані та інформація. Вміст у базі даних, сховищі файлів тощо.

Такий розподіл спрощує уявлення про формування системи безпеки хмарних послуг, адже різні фокуси безпеки відображаються на різних логічних рівнях.

Безпека додатків зіставляється із структурою додатків, безпека даних з інфоструктурою та безпека інфраструктури з інфраструктурою.

Хмарні обчислення значно відрізняються від традиційних на кожному з представлених рівнів, проте найбільш вагомими особливостями виділяється метаструктура - хмарна метаструктура включає в себе компоненти рівня керування, які підтримуються в мережі та доступні віддалено. Ще одна ключова відмінність полягає в тому, що в хмарі, як правило, подвоюється кожен логічний шар. Інфраструктура, наприклад, включає як інфраструктуру, яка використовується для створення хмари, так і віртуальну інфраструктуру, яка використовується та керується споживачем хмари. У приватній хмарі одна й та сама організація може керувати обома; у загальнодоступній хмарі постачальник керує фізичною інфраструктурою, а споживач керує своєю частиною віртуальної інфраструктури [6, с. 19].

1.2 Різновиди хмарних обчислень та їх особливості

Існуючі поняття хмарних технологій можуть відрізнятись у формулюваннях, проте можна узагальнити деякі ключові характеристики, які зображені на рис. 2.

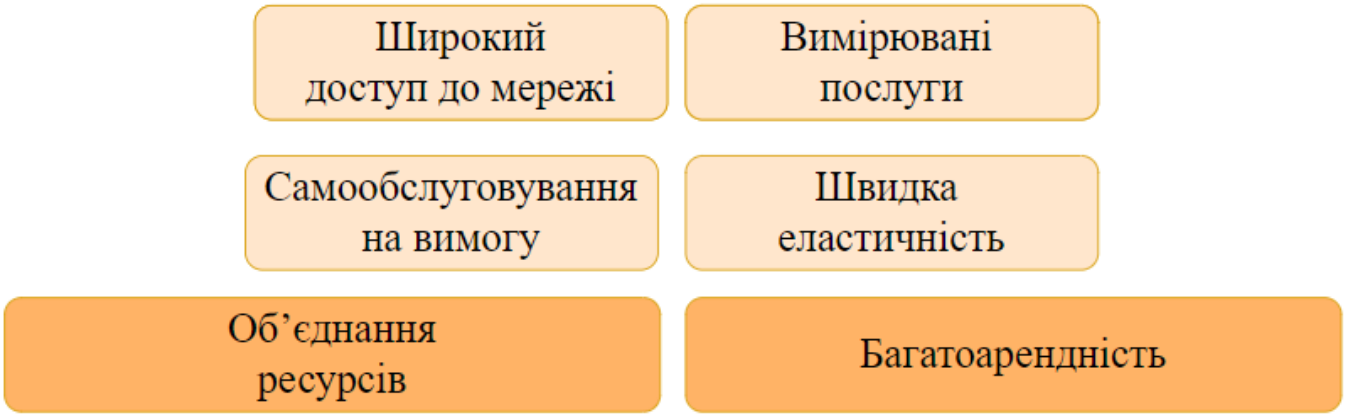

Рисунок 2 - Основні характеристики хмарних обчислень

Самообслуговування на вимогу означає те, що споживач може самостійно отримувати обчислювальні можливості, без потреби звертатись до їх постачальника.

Швидка еластичність передбачає здатність хмари до швидкого та еластичного (теоретично необмеженого) масштабування в будь-який час, в міру зростання попиту.

Широкий доступ до мережі надає можливість використовувати хмару як через тонких, так і через товстих клієнтів, без необхідності фізичного доступу до ресурсів. Проте мережа не є обов'язковою частиною послуги.

Вимірювані послуги автоматично контролюють та оптимізують використання ресурсів, яке можна легко контролювати.

Об'єднання ресурсів – це фундаментальна особливість хмарних обчислень. Постачальники забезпечують обслуговування кількох споживачів за допомогою фізичних та віртуальних ресурсів, які динамічно розподіляються відповідно до потреб споживачів [7].

Багатоарендність (або мультитенантність) є доповненням до загальноприйнятих характеристик, проте також може вважатись однією з основних (для публічної хмари). Вона відрізняється від попередньої ознаки, адже наголошує на тому, що кілька різних груп споживачів мають спільні ресурси, проте вони сегреговані та ізольовані один від одного. Сегрегація дозволяє постачальнику хмари розділяти ресурси на різні групи, а ізоляція гарантує, що вони не зможуть бачити або змінювати активи один одного.

Дві останні характеристики є найбільш корисними особливостями хмарних обчислень і водночас найбільш небезпечними з точки зору безпеки, адже замовник в такому випадку не може контролювати свої ресурси і відповідальність за забезпечення їх ізоляції повністю лежить на надавачу хмарних послуг.

Такі особливості технологій хмарних обчислень дозволяють реалізувати безумовні переваги хмарних сервісів над традиційними інформаційними системами, завдяки яким хмара набуває популярності з кожним роком. До головних переваг, зокрема, належать можливість мобільного доступу до хмарних сервісів через зручний інтерфейс у будь-який час, з будь-якого місця, швидке розгортання та економія коштів, які більше не потрібно витрачати на обладнання й електроенергію, обслуговуючий персонал і додаткові ліцензії – натомість користувачі майже одразу

отримують високопродуктивні ресурси з професійними рішеннями, теоретично необмеженою ємністю зберігання та нульовими початковими інвестиціями [8]. До цього переліку входить також здатність швидко адаптуватися до змін у бізнес-середовищі, а також гарантія безперервності бізнесу завдяки резервному копіюванню даних, розподілу серверів та ефективним планам аварійного відновлення після збоїв. Більше того, НХП надають користувачам доступ до автоматичних оновлень і розширених функцій безпеки, які гарантують безпечне зберігання та обробку даних.

1.2.1 Моделі розгортання хмарних обчислень

При виборі безпечного рішення для хмарних обчислень основним питанням є тип хмари, який буде запроваджено. На даний момент пропонується чотири типи моделей розгортання хмари [8]:

Публічна хмара – хмарна інфаструктура в ній надається широкому загалу або великій галузевій групі та належить організації, що продає хмарні послуги. Основною характеристикою публічної хмари є багатоарендність, яка може бути досягнута за допомогою віртуалізації на різних рівнях програмного стеку. Це найпопулярніша модель, яка є найбільш економічно вигідною, але менш безпечною, порівняно з іншими, тому ключове питання керівництва, на яке потрібно відповісти в рамках Service Level Agreement (далі - SLA), стосується забезпечення достатнього контролю безпеки та спільної відповідальності [9].

У приватній хмарі масштабовані ресурси та віртуальні програми, надані постачальником хмари, доступні тільки організації та визначеним зацікавленим сторонам. Він відрізняється від загальнодоступної хмари тим, що всіма хмарними ресурсами та додатками керує сама організація, подібно до функціональних можливостей інтранету. Цей тип хмар гарантує найкращий контроль над безпекою, адже він забезпечує більший контроль підприємства над розгортанням і використанням, а також гарантує спеціальну внутрішню доступність, проте така модель розгортання є значно дорожчим варіантом.

Громадська хмара використовується кількома організаціями та підтримує певну спільноту, яка має спільні проблеми, однакові або взаємні вимоги. Вони спеціально створені для певної мети, щоб сумісні організації могли спільно використовувати хмарне середовище для роботи над спільними проектами.

Гібридна хмара – це комбінація з кількох хмар, які пов'язані між собою стандартизованою або запатентованою технологією, що забезпечує переносимість даних і додатків (наприклад, розрив хмари для балансування навантаження між хмарами). Гібрид також зазвичай використовується для опису нехмарного центру обробки даних, підключеного безпосередньо до хмарного постачальника. Гібридна хмара ідеально підходить для забезпечення безпеки, гнучкості та масштабованості, адже включає можливості як публічної хмари, так і приватної. Таким чином, організації можуть гарантувати конфіденційність своїх даних у приватній хмарі та одночасно тестувати програму в загальнодоступній, де безпека не є критично важливою умовою.

Моделі розгортання визначаються на основі споживача хмари , тобто того, хто використовує хмару. Як показано на рис. 3, організація, яка володіє та керує хмарою, може відрізнятися навіть у межах однієї моделі розгортання.

	Адміністратор інфраструктури	**Власник інфраструктури**	**Розташування інфраструктури**	**Користувачі**
Публічна хмара	Надавач послуг	Надавач послуг	За межами організації	Ненадійні
Приватна/ громадська	Користувач / Надавач послуг	Користувач / Надавач послуг	Локально / За межами	Надійні
Гібридна хмара	Користувач & надавач послуг	Користувач & надавач послуг	Локально & за межами організації	Надійні & ненадійні

Рисунок 3 - Моделі розгортання хмарних обчислень

1.2.2 Сервісні моделі хмарних обчислень

Після вибору моделей розгортання хмари, наступне міркування безпеки стосується різних моделей хмарних послуг. При цьому слід звертати увагу на так звані кордони управління – тобто на тому, чим, у порівнянні з традиційними моделями розгортання у власній інфраструктурі, можна керувати при переході на хмарну платформу. Архітектуру хмарних обчислень можна класифікувати за трьома основними типами сервісних моделей, як зображено на рис. 4.

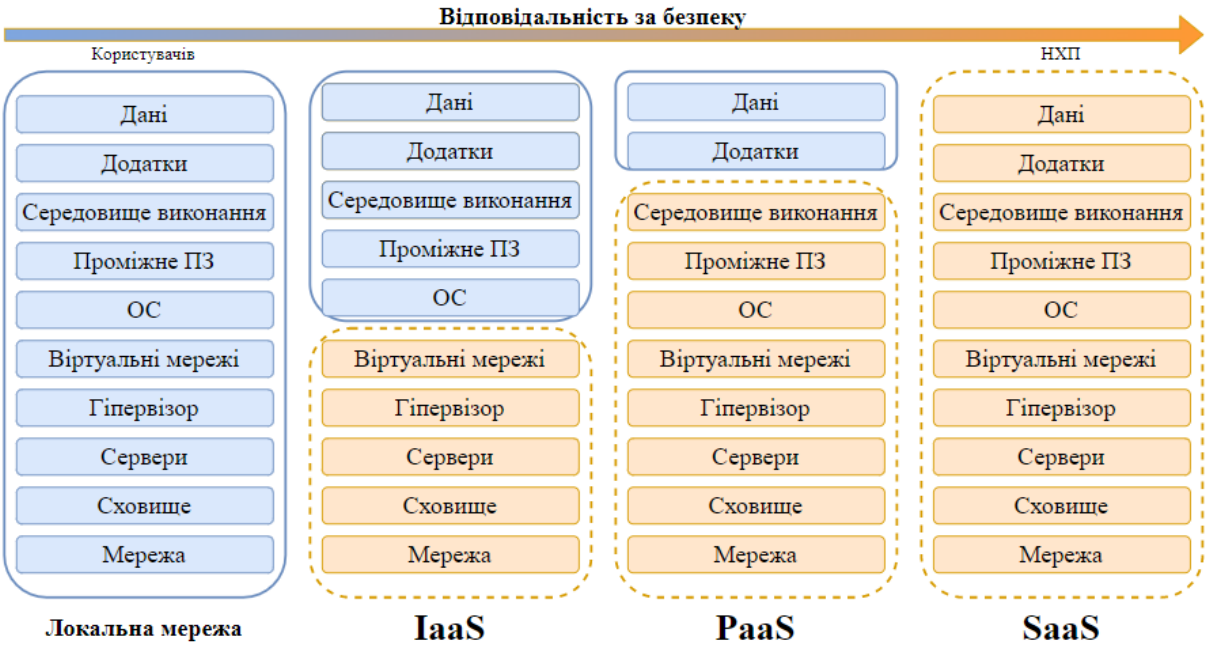

Рисунок 4 - Основні моделі хмарних послуг

Інфраструктура як послуга (далі - IaaS) - пропонує користувачам доступ до пулу ресурсів фундаментальної обчислювальної інфраструктури, такої як сервери, мережеві пристрої та обчислювальна потужність. При цьому споживач не контролює базову хмарну інфраструктуру, але має контроль над операційними системами, сховищем, розгорнутими програмами та обмеженим контролем окремих мережевих компонентів (наприклад, брандмауерів хоста). Такий підхід зводить до мінімуму потребу у величезних початкових інвестиціях у комп'ютерне обладнання і персонал, а також забезпечує різний ступінь фінансової та функціональної

гнучкості, якої немає у внутрішніх центрах обробки даних, оскільки обчислювальні ресурси можна додавати або вивільняти за потребою набагато швидше та рентабельніше.

Платформа як послуга (далі - PaaS) забезпечує додатковий рівень «орендованих» функціональних можливостей - за допомогою PaaS користувач не керує базовою хмарною інфраструктурою, але контролює розгорнуті програми та обмежені конфігурації середовища розміщення сервісів. PaaS абстрагує та надає платформи для розробки (наприклад, місце для запуску програмного коду) або додатки, такі як бази даних.

Програмне забезпечення як послуга (далі - SaaS) - це повноцінний додаток, яким повністю керує НХП – він контролює базову інфраструктуру та навіть можливості окремих додатків, за винятком обмежених налаштувань конфігурації програм, що стосуються користувача. Доступ до програм здійснюється через тонкий клієнтський інтерфейс, наприклад, за допомогою веб-браузера та мобільних додатків. SaaS надає обмежену функціональність, це спрощує управління, зменшує відповідальність, проте значно збільшує ризики з безпеки. В даній моделі безпека веб-сервісів є життєво важливою умовою – необхідно враховувати шифрування розширюваної мови розмітки (XML), рівень безпечних сокетів (SSL) та інші доступні параметри, які використовуються для забезпечення захисту даних, що передаються через Інтернет.

1.3 Ландшафт загроз безпеки хмарних сервісів

Згідно з останнім прогнозом Gartner, Inc., очікується, що до 2025 року понад 85% організацій приймуть принцип «Cloud First» і не зможуть повністю реалізувати свої цифрові стратегії без використання хмарних послуг [10]. Таке широке прийняття технологій хмарних обчислень, означає, що цифрові або продуктові команди будуть використовувати архітектурні принципи та можливості хмарних сервісів, щоб скористатися перевагами хмарного середовища. Разом з тим, хмарні сервіси залишають за собою деякі загрози для даних користувачів. Нижче

представлений перелік найпоширеніших загроз інформаційній безпеці при використанні хмарних послуг [11; 12].

1. Втрата даних може відбуватися різними способами. Дані можуть бути скомпрометовані через видалення, модифікацію, втрату ключа шифрування та іншими способами, такими як стихійні лиха тощо. Організації повинні підтримувати комплексне резервне копіювання своїх даних та запровадити надійні процедури управління ключами, щоб уникнути таких загроз.

2. Витік даних – це отримання конфіденційної інформації неавторизованим користувачам. Витік даних може статись через неправильні механізми аутентифікації та авторизації, порушення контролю доступом і ролями, ненадійне використання ключів шифрування, проблеми з остаточним видаленням або збій операційної системи.

3. Викрадання облікового запису, послуг або трафіку відбувається, якщо зловмисник отримує доступ до облікових даних для входу, тоді зламаний обліковий запис може бути базою для викрадання даних користувачів, маніпулювання інформацією, зловмисник також може перенаправляти споживача на нелегітимні сайти та запускати різні атаки, в тому числі й для подальшої ескалації привілеїв.

4. Небезпечні прикладні програмні інтерфейси (Application Programming Interface, далі - API), тобто інтерфейси, що є стандартами та протоколами, які споживачі використовують для підключення до хмарних служб. Вони повинні мати безпечні стандарти сертифікації, належний контроль доступу, надійну автентифікацію, шифрування та механізми моніторингу активності, щоб уникнути таких загроз, як анонімний доступ, автентифікація з відкритим текстом, багаторазові токени або паролі, неправильна авторизація, обмежений моніторинг та можливості логування.

5. Шкідливі інсайдери є довіреними людьми в організації, які мають доступ до конфіденційних активів. Вони можуть виконувати непривілейовані дії, щоб проникнути в активи організації, а також завдати репутаційної шкоди бренду та фінансових втрат, виконуючи різні дії, які брандмауер або система виявлення вторгнень (далі - IDS) будуть вважати за легальну діяльність. У цьому випадку для

безпеки хмарних сервісів необхідні прозорість загальної практики інформаційної безпеки, звітів про відповідність, сповіщень про порушення та комплексна перевірка постачальників.

7. Зловживання хмарними сервісами можна охарактеризувати як неетичні та незаконні дії споживача щодо неправомірного використання послуг. Недорога інфраструктура, високий рівень ресурсів, слабкі процедури реєстрації сприяли анонімності спамерам, злочинцям та іншим зловмисникам, які проникають у загальнодоступну хмару, знаходять спосіб завантажити шкідливе програмне забезпечення (далі - ШПЗ) на тисячі комп'ютерів і використовувати потужність хмарної інфраструктури для атаки на інші машини.

Для зменшення такої загрози необхідно впроваджувати більш суворі процеси реєстрації, проводити комплексну інтроспекцію трафіку клієнтів та моніторити загальнодоступні чорні списки для перевірки власних мереж.

8. Вразливості спільної інфраструктури виникають у мультиарендній структурі, де послуги на вимогу надаються за допомогою спільних ресурсів між різними користувачами, які мають доступ до однієї віртуальної машини. Вразливості у віртуалізованих гіпервізорах дозволяють зловмисникам отримувати неналежний доступ і контролювати віртуальні машини інших споживачів. Для того, щоб уникнути цих загроз, необхідно забезпечити ізоляцію користувачів, сприяти надійній автентифікації та контролю доступу, постійно моніторити хмарне середовище, проводити сканування вразливостей і аудит конфігурацій.

Не можна виключати загрози для фізичного обладнання, яке може бути пошкоджено або зазнати збоїв, загрозу порушення периметрів безпеки провайдерів хмарних послуг, проблем, що можуть виникати при зміні бізнес-моделі або припиненні дії угоди між користувачем та надавачем хмарних послуг, використанні послуг різних хмарних провайдерів тощо.

Існує також небезпека щодо дотримання правових і нормативних вимог, яким повинні відповідати як користувачі, так і надавачі хмарних послуг. Це питання є ключовим в контексті даної роботи, адже при використанні технологій хмарних обчислень користувачі не мають можливості повноцінно контролювати всі

процедури безпеки і наражаються на невідомий профіль ризику, що може спричинити серйозні загрози, а запобігти цьому можна лише споживаючи послуги надійних сертифікованих провайдерів хмарних послуг.

Розглянуті загрози конгруентні з основними загальновизнаними вимогами до захисту хмарних сервісів. При цьому вимоги, яких сторони повинні дотримуватися, залежать від інфраструктури, яку планується використовувати, тому тільки поєднуючи різні типи розгортання хмар з моделями доставки, ми отримуємо цілісну ілюстрацію до вимог з безпеки хмарних обчислень, як показано на рис. 5 [13].

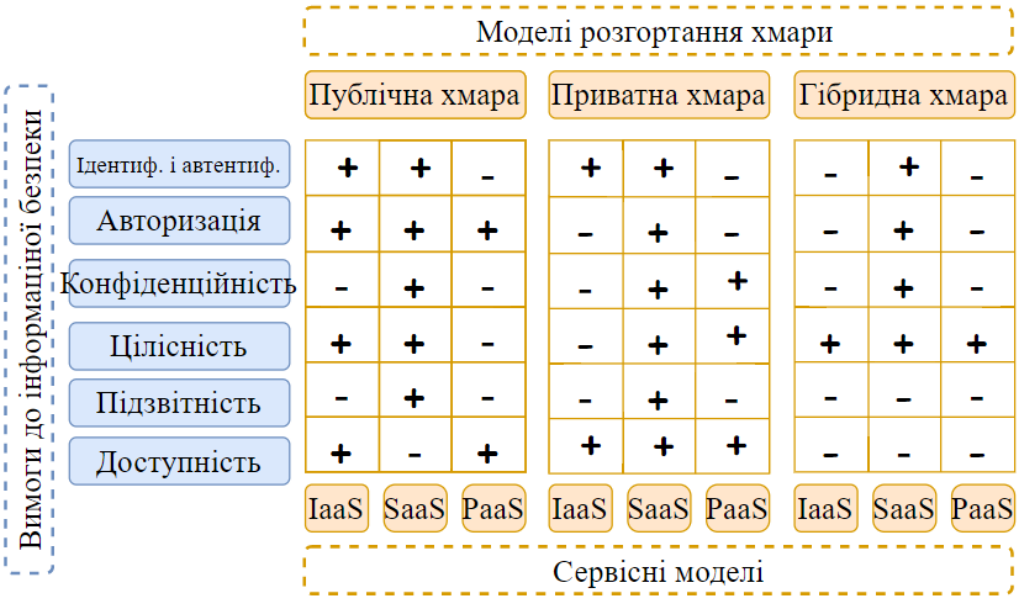

Рисунок 5 - Вимоги до безпеки хмарних обчислень

На рис. 5 різні моделі хмарної доставки та моделі розгортання співвідносяться з вимогами інформаційної безпеки, де «+» позначає критичні й обов'язкові вимоги, а «-» -додаткові. Така схема містить наступні вимоги:

1) Ідентифікація та автентифікація призначені для перевірки та підтвердження окремих користувачів хмари на базі наданих для них повноважень для доступу до будь-яких даних через хмару. Ці процеси спрямовані на уникнення несанкціонованого доступу до ресурсів користувачів.

2) Авторизація є важливою вимогою інформаційної безпеки в хмарних обчисленнях для забезпечення того, що користувачі, які надіслали запит на конкретну інформацію, мають права до її доступу.

3) Конфіденційність передбачає збереження даних користувачів і надання доступу до даних лише визначеним особам. Підтвердження конфіденційності профілів користувачів і захист їхніх даних, до яких здійснюється віртуальний доступ, дозволяє застосовувати протоколи інформаційної безпеки на різних рівнях хмарних додатків. До цієї вимоги також можна включити анонімність, тобто вся інформація, яка може бути використана для ідентифікації власника або поточного користувача, за замовчуванням має бути конфіденційною і не розповсюджуватися.

4) Цілісність означає гарантування того, що дані не змінюються або модифікуються під час їх зберігання або транспортування, і лише авторизовані користувачі мають доступ до зміни, модифікації, копіювання або видалення.

5) Доступність гарантує забезпечення доступу до інформації в хмарні та пов'язаних з нею користувачів за мірою необхідності в будь-який час.

6) Підзвітність дозволяє фіксувати діяльність користувачів, гарантувати автентичність, неспростовність інформації через надання маркерів для передачі даних у хмарних додатках, таких як цифрові підписи, позначки часу та служби підтвердження.

Надану схему потрібно розглядати як орієнтир при оцінці рівня безпеки хмарних провайдерів для дослідження оптимального балансу, необхідного для захисту технологій хмарних обчислень, проте, звичайно, її можна доповнити іншими властивостями за потреби.

Висновки за розділом 1

В даному розділі було висвітлено поняття хмарних обчислень та хмарних сервісів, а також перераховано учасників відносин при користуванні хмарою відповідно до законодавства України. Розгляд характерних особливостей такого

типу систем пояснює, в чому полягають переваги хмарних сервісів, які зумовлюють їх надзвичайну популярність серед різних типів користувачів.

Окрім цього, було досліджено різноманіття сервісних моделей і моделей розгортання хмар, перераховано їх переваги і недоліки.

Також було розглянуто основні загрози, характерні для хмарних сервісів, на основі яких побудовано та проілюстровано схему вимог до безпеки різних видів хмар, що доводить актуальність питання оцінки відповідності НХП вимогам безпеки.

РОЗДІЛ 2
НОРМАТИВНО-ПРАВОВЕ ПІДГРУНТЯ ХМАРНИХ ТЕХНОЛОГІЙ

2.1 Типи нормативних актів із використання хмари

Стандарти інформаційної безпеки — це еталонний набір найкращих практик, створених експертами для захисту організацій від загроз інформаційній безпеці та покращення їхньої позиції кібербезпеки. Вони можуть слугувати міцною основою як для початкової розробки, так і вдосконалення системи безпеки існуючого інформаційного середовища, виправдовуючи час та витрати при запровадженні додаткових засобів контролю безпеки.

При цьому програми оцінювання та атестації відповідності стандартам, які пропонують спосіб вимірювання продуктів і послуг за об’єктивними критеріями, забезпечують високий рівень безпеки даних та надають конкурентні переваги при порівнянні запропонованих послуг. Це значно спрощує вибір надавачів хмарних послуг для користувачів і може слугувати гарантом якості систем, що сприятимуть уникненню фінансових втрат у результаті порушення безпеки, зможуть повноцінно забезпечувати конфіденційність та цілісність даних, відповідність нормативним вимогам, а також допоможуть визначати відповідальність щодо обробки інформації.

Еволюційна парадигма надання хмарних послуг зумовила необхідність у створенні ефективної бази нормативних документів, які містять у собі повний опис обов’язкових стандартизованих процедур, що можуть гарантувати користувачам безпеку при впровадженні хмарних технологій та користуванні хмарними послугами.

Велика кількість стандартів може здаватись складною для сприйняття, тому перш ніж ознайомитись із основами функціонування хмарних технологій на законодавчому та правовому рівні, необхідно розглянути їх ієрархію [5]. Систематизований розгляд поточних стандартів залежно від рівня суб’єктів стандартизації, що їх затвердив, представлений на рис. 6.

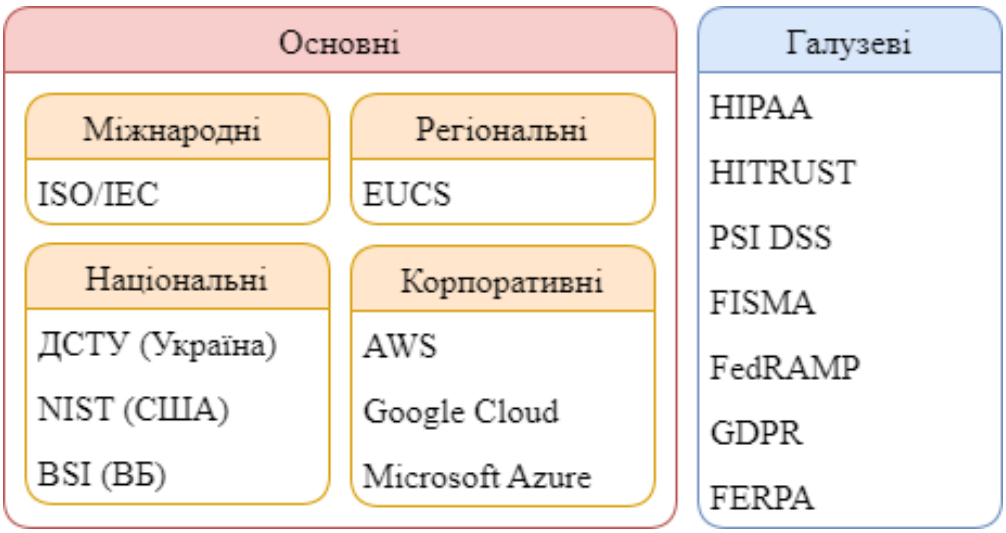

Рисунок 6 - Ієрархія стандартів залежно від рівня суб’єктів стандартизації

Варто зазначити, що стандарти знаходяться в спектрі між де-юре, тобто ті, що визначені формально і суворо регулюються, і де-факто – це загальноприйняті методи чи продукти, які проте є неформальними. Наприклад, документи окремих компаній (корпоративні, див. рис. 6) можуть розглядатись як стандарти тільки де-факто.

Дослідивши різноманіття стандартів з різних джерел, прослідковується закономірність проблем впровадження хмарних рішень, згідно з якої можна класифікувати документи на деякі види, враховуючи специфіку об’єкта стандартизації як представлено на рис. 7.

Рисунок 7 - Класифікація стандартів відповідно до об'єкта регулювання

Найважливішим класом хмарних стандартів із найяскравішими доказами широкого застосування є стандарти безпеки. Вони і будуть об’єктом дослідження даного розділу. Нижче представлений розгляд основоположних документів, які мають визначальну роль у функціонуванні хмарних сервісів та забезпеченні їх безпеки.

2.2 Аналіз стандартів із хмарної безпеки від ISO

Спільними зусиллями представників ISO та Міжнародної електротехнічної комісії (далі - IEC), які займаються питаннями пов'язаними зі стандартами в галузі інформаційних технологій, були розроблені стандарти для багатьох видів систем і технологій, у тому числі для хмарних середовищ. Ці документи складають цілу систему – вони доповнюють один одного в різних складових хмарних технологій і забезпечують їх безпеку на кожному рівні функціонування. Загальний ландшафт стандартів ISO/IEC при роботі з хмарою та взаємозв’язки між ними представлений на рис. 8.

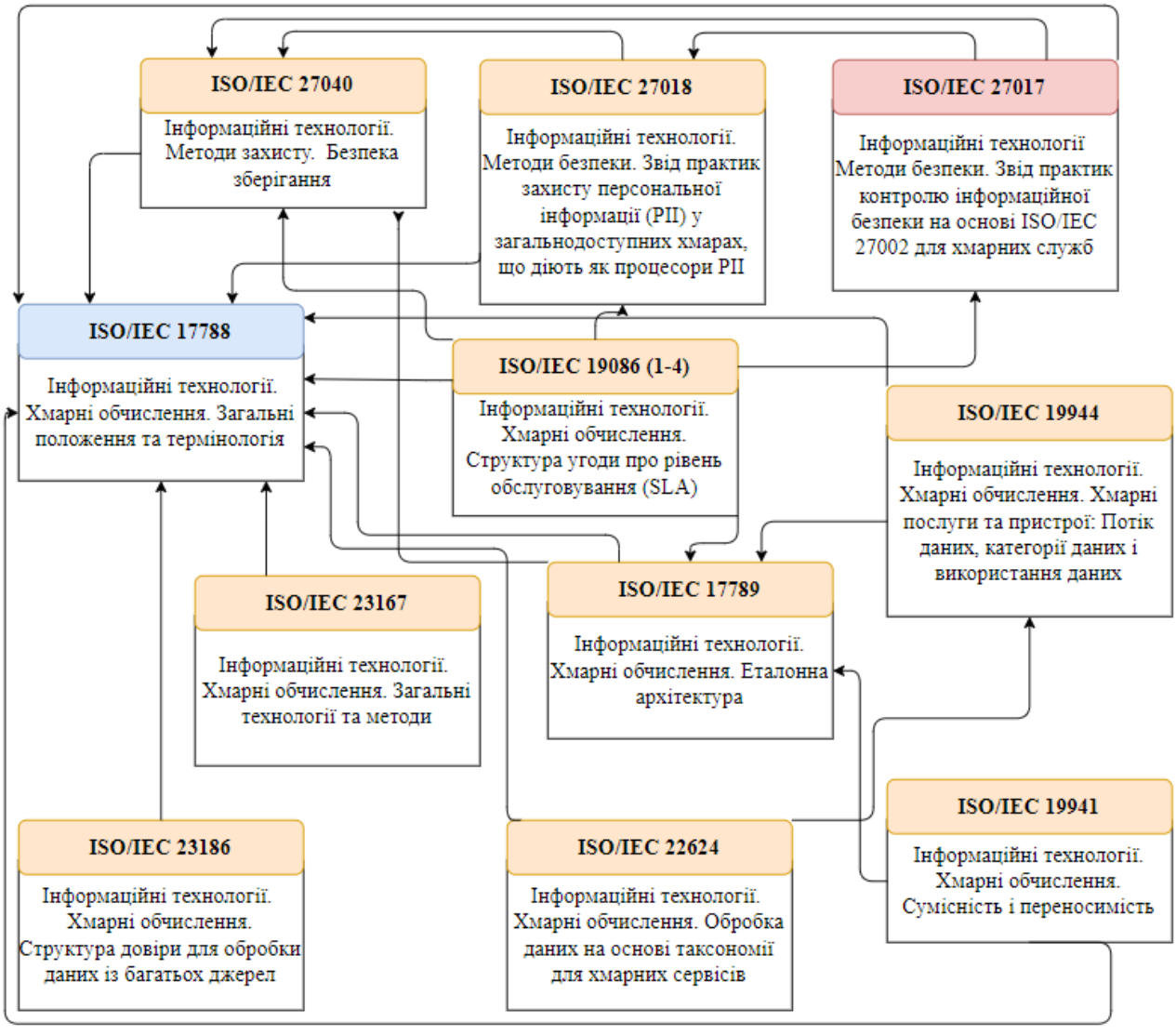

Рисунок 8 - Взаємозв’язок між стандартами ISO/IEC з хмарних обчислень

Серед представлених документів, базовими стандартами для хмарної безпеки можна вважати сімейство стандартів ISO/IEC 27000. Їх використання дозволяє організаціям будь-якого виду керувати безпекою активів, таких як фінансова інформація, інтелектуальна власність, дані співробітників або інформація, довірена третім сторонам.

1. ISO/IEC 27001 “Information technology — Security techniques — Information security management systems — Requirements” – описує вимоги, що надають основу та рекомендації для створення системи управління інформаційною безпекою, яка застосовна до хмарних і нехмарних програм. Це також основа для проведення аудитів безпеки в хмарі [14].

2. ISO/IEC 27017 “Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002” - технічна специфікація, яка надає рекомендації щодо безпеки в хмарі, які можуть допомогти організаціям підходити до хмарної безпеки більш систематично та надійно [15]. Стандарт створений на основі ISO/IEC 27002, який описує 37 засобів контролю, що можуть бути встановлені для відповідності стандарту ISO-27001 із додаванням 7 додаткових елементів з урахуванням специфіки хмарних середовищ [16]. Ці додаткові компоненти визначають ролі й відповідальність між постачальниками хмарних послуг та їх користувачами, надають адміністративні можливості відслідковувати активність хмарних мереж, описують захист та розподіл віртуальних обчислювальних середовищ клієнтів, конфігурацію віртуальних машин, узгодженість управління безпекою для хмарних обчислень, віртуальних і фізичних мереж, а також умови повернення активів при припиненні договору.

3. ISO/IEC 27018 “Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors” - надає рекомендації щодо забезпечення конфіденційності персональної інформації в спільних хмарних середовищах [17].

Вимоги міжнародних стандартів від ISO вважаються найбільш впливовими та жорсткими, тому часто вони стають основою для державних стандартів України.

Адже виконання вимог цих стандартів, що ґрунтуються на багаторічному досвіді різних країн гарантує високу якість та надає можливість реалізації продуктів і послуг на світовому ринку.

2.3 Аналіз стандартів із хмарної безпеки від NIST

Національний інститут стандартів і технологій США широко підтримує розвиток технологій та бере участь у створенні стандартів і специфікацій як для державного використання, так і в приватному секторі. Напрацювання NIST, зокрема ті, що стосуються хмарних обчислень широко використовуються не тільки в США, а й враховуються при розробці міжнародних стандартів. Загальний вигляд сукупності публікацій NIST, які мають безпосереднє відношення до безпеки хмарних обчислень можна зобразити в схематичному зображенні як на рис. 9.

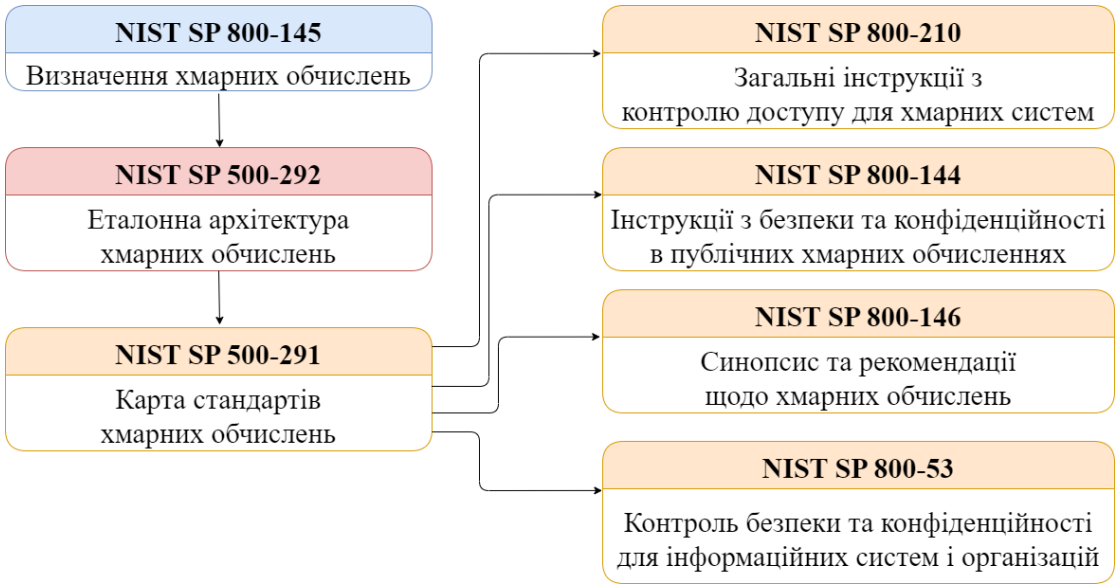

Рисунок 9 - Схема стандартів NIST з хмарної безпеки

Фундаментальним документом в цій сфері можна вважати NIST SP 800-145, NIST Definition of Cloud Computing [2]. Стандарт описує важливі аспекти хмарних обчислень і служить еталоном для порівняння хмарних послуг і стратегій розгортання. Це також є основою для обговорення хмарних обчислень і способів їх використання.

NIST SP 500-292, NIST Cloud Computing Reference Architecture – ключовий документ, який визначає еталонну архітектуру хмарних технологій, в тому числі й основний набір компонентів безпеки, які можуть бути реалізовані для захисту хмарного середовища [7].

Карту основних стандартів, застосовних до забезпечення безпеки хмарних технологій, відповідно до спеціальної публікації NIST 500-291, NIST Cloud Computing Standards Roadmap, можна поділити на декілька категорій – Автентифікація та авторизація, Конфіденційність, Цілісність, Управління ідентифікацією, Моніторинг безпеки та Реагування на інциденти, Контроль безпеки, Доступність, Управління політикою безпеки [18]. Цей документ надає своєрідну компіляцію доступних стандартів від різних організацій разом із маркуванням їхнього статусу – «Затверджений», «Тестується» та «Доступний для ринку».

До хмари також можна застосувати потужний інструмент NIST Cybersecurity Framework (далі - CSF), який складається зі стандартів, рекомендацій і найкращих практик для управління ризиками, пов’язаними з кібербезпекою [19]. NIST CSF пропонує просту, але ефективну модель, яка включає п’ять ключових функцій кібербезпеки, щоб організувати рекомендовані засоби контролю безпеки в робочі потоки, які зображені на рис. 10. Користувачі хмарних послуг можуть використовувати цю структуру для планування стратегій безпеки для оптимального захисту своїх даних.

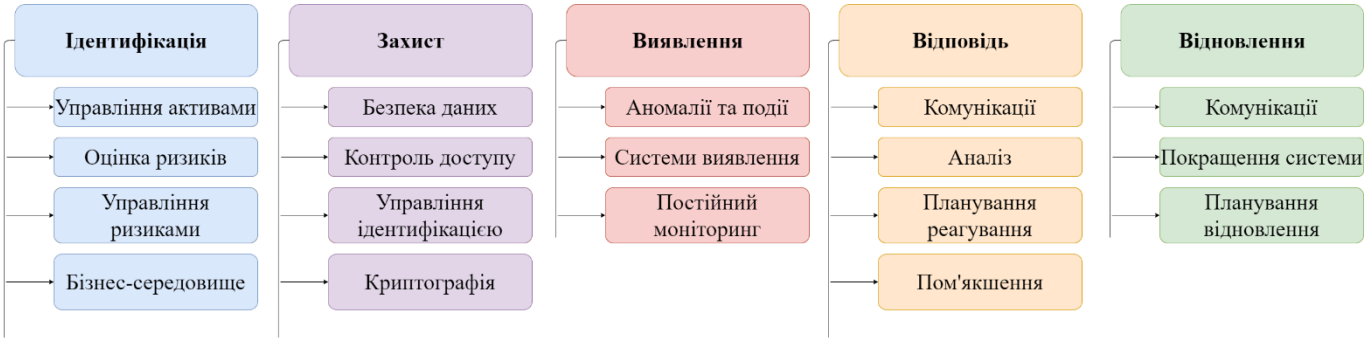

Рисунок 10 - Структура кібербезпеки NIST

Функція «Ідентифікація» передбачає розвиток організаційного розуміння для управління ризиками кібербезпеки для систем, активів, даних і можливостей. Функція «Захист» покликана розробити та впровадити відповідні запобіжні заходи для забезпечення надання послуг критичної інфраструктури. «Виявлення» - розробити та запровадити відповідні дії для виявлення події кібербезпеки. «Відповідь» відповідає за розробку й впровадження відповідних заходів щодо виявленої події кібербезпеки. А функція «Відновлення» необхідна щоб розробити та запровадити відповідні дії для вжиття заходів після виявленої події кібербезпеки.

2.4 Особливості галузевих стандартів

При оцінюванні відповідності не можна не взяти до уваги вимоги інформаційної безпеки галузевих стандартів – вони допомагають врахувати особливості окремих сфер діяльності з метою створення додаткових умов із забезпечення безпеки даних, що можуть стати ключовими для підприємства.

Наприклад, правило безпеки HIPAA встановлює стандарти для збереження конфіденційності та безпеки електронної особистої медичної інформації та вимагає надання трьох видів гарантій - адміністративних, фізичних і технічних [20]. HIPAA вимагає від усіх організацій охорони здоров’я демонструвати й документувати регулярне сканування загроз для оцінки медичних пристроїв, програм і мереж на наявність вразливостей, зловживань та слабких місць безпеки. Крім того, HIPAA вимагає від охоплених організацій оцінити ймовірність та вплив потенційних ризиків для чутливої медичної інформації та впровадити та задокументувати відповідні заходи безпеки для вирішення цих зон ризику. Загалом, служба охорони здоров’я та соціальних служб вимагає, щоб дані були захищені від «розумно очікуваних загроз безпеці чи цілісності інформації», а також підтримували «постійний, розумний та відповідний захист безпеки».

Стандарт безпеки даних індустрії платіжних карток (далі - PCI-DSS) — це галузевий мандат, який визначає мінімальні засоби контролю безпеки, необхідні для захисту даних власників карток клієнтів протягом усього періоду роботи [21]. PCI-

DSS є обов’язковим до виконання при роботі з міжнародними платіжними системами, зокрема VISA, JCB та MasterCard для гарантій захисту від крадіжки клієнтської інформації та шахрайства під час транзакцій. PCI DSS зокрема зобов’язує, що будь-яка компанія, яка зберігає, обробляє або передає дані власника картки, передбачає використання антивірусного ПЗ, установку брандмауерів та проведення регулярних тестувань на вразливості.

Велику вагу в захисті державних даних і мінімізації ризиків інформаційної безпеки в рамках федеральних систем даних при переході уряд до комерційних хмарних послуг мають галузеві федеральні стандарти уряду США - Федеральна програма управління ризиками та авторизацією (далі - FedRAMP) [22] і Федеральний закон про управління інформаційною безпекою (далі - FISMA). Усі федеральні організації, які використовують або планують використовувати хмарні послуги, зобов’язані впроваджувати ці програми, адже вони надають стандартну методологію оцінки безпеки, авторизації та постійного моніторингу хмарних продуктів і послуг та є надійною системою відповідності, яка вимагає від усіх федеральних агенцій і їхніх підрядників захищати інформаційні системи та активи.

Відомий як один із найсуворіших законів про конфіденційність даних у всьому світі, Загальний регламент захисту даних (далі - GDPR) – загальновизнаний стандарт із регулювання захисту даних та конфіденційності для Європейського Союзу і його виконання вважається обов’язковим для компаній, що обробляють будь-які персональні дані громадян чи резидентів ЄС або пропонують товари й послуги [23].

Таким чином, часто користувачам доводиться орієнтуватись не тільки на загальні принципи забезпечення захисту інформації, що циркулює на підприємстві, а й додатковими вимогами, що зумовлені особливостями їхньої сфери діяльності.

2.5 Особливості українського законодавства щодо хмарних технологій

Відповідно до рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» та пункту

65 даного плану про забезпечення належної правової моделі функціонування кіберпростору, 17 лютого 2022 року було прийнято Закон України №2075-IX «Про хмарні послуги», який набуває чинності після шести місяців після його опублікування через необхідність розробки ряду підзаконних нормативно-правових актів і впровадження можливостей хмарних технологій [4]. Закон вводить нову для українського законодавства термінологію, що пов'язана з хмарними сервісами, регулює правовідносини щодо обробки та захисту даних при використанні технології хмарних обчислень і наданні хмарних послуг, а також описує особливості користування хмарними послугами серед органів державної влади. Даний нормативно-правовий акт закладає засади цифрової трансформації України і створює базу для реалізації державної стратегії Cloud First.

Cloud First Strategy успішно впроваджують провідні країни світу починаючи з 2011 року. Вона передбачає поступову відмову від традиційного апаратного забезпечення і фізичних серверів та надання пріоритету хмарним рішенням при здійсненні державних закупівель в управлінській сфері, закладах освіти та науки, а також інших сферах діяльності, що, в свою чергу, має створити сприятливі передумови ефективної взаємодії суспільства і держави. В умовах військового стану, коли тиск зовнішніх та внутрішніх загроз посилюється неодноразово, питання законодавчого врегулювання відносин між провайдерами і користувачами хмарних сервісів є особливо актуальним, тому що локальні датацентри виявляються вразливими як ніколи.

Прийняття такого закону є економічно обґрунтованим рішенням. Після проведення аудиту державних закупівель, автори законопроекту передбачили, витрати на ІТ-закупівлі в період з 2020 по 2024 роки досягнуть 100 млрд грн [24]. Якщо ж стратегію Cloud First вдасться реалізувати хоча б частково і половина потреб в сфері інформаційних технологій буде забезпечуватись через використання хмарних послуг, а не капітальних інвестицій, то загальна економія бюджетних коштів може сягати 40 млрд грн за цей самий період часу.

Окрім цього, використання хмарних технологій в державних установах може стати ефективним механізмом боротьби з корупцією, адже це знижує ризики

фінансових махінацій при закупівлі обладнання і сприяє максимальній прозорості діяльності органів державної влади.

Робота над цим законопроектом тривала з 2019 року і зустріла чимало критики, адже крім очевидного прогресу, такий підхід приховує в собі деякі ризики - ухвалення Закону передбачає повне розкриття інформаційних кордонів, адже надає право на обробку державних даних іншим юрисдикціям, що виключає можливість «цифрового суверенітету» України. Більше того, на думку деяких луддитів, запропонована стратегія виглядає як лобіювання певного виду технологій на державному рівні [25].

Закон «Про хмарні послуги» забороняє обробляти інформацію, що становить державну таємницю, державні та єдині реєстри, або службову інформацію за допомогою хмарних ресурсів та ЦОД, які:

- розташовані за межами України
- розташовані на тимчасово окупованій території
- розташовані на території держави-агресора
- належать підсанкційним фізичним чи юридичним особам.

Перший пункт, на мою думку, є складними до виконання і може бути необов’язковим, адже міжнародні передачі таємної інформації не заперечуються як Законом «Про державну таємницю», так і Законом «Про службову інформацію» на підставі міжнародних договорів.

Окрім цього, зазначені вимоги не дозволяють надавачу хмарних послуг використовувати будь-які технічні засоби, які розміщуються на території, де тимчасово втратили повноваження органи державної влади України, в межах держави-окупанта, або ж ті, якими володіють суб’єкти, які потрапили під санкції.

Навіть Закон України «Про державне регулювання діяльності щодо організації та проведення азартних ігор» [26] забороняє використання технічних засобів, які знаходяться поза межами України для проведення азартних онлайн-ігор, а обробка інформації повинна здійснюватися виключно на території держави. Це також потрібно враховувати при використанні послуг хмарних провайдерів.

Як зазначено в Законі, надавачі хмарних послуг повинні бути зареєстровані в офіційному переліку, який контролює спеціально створений орган - регулятор комунікаційних послуг за визначеною процедурою, після перевірки переліку необхідних документів. Це гарантує виконання вимог, передбачених статтею 8 цього Закону про необхідність забезпечувати високий рівень безпеки інформаційних систем і мереж, який гарантує безпеку систем та устаткування, елементи інформаційної системи для моніторингу й врегулювання інцидентів, забезпечує управління безперервністю бізнесу, проведення аудитів та випробувань, а також враховує відповідність міжнародним стандартам;

Цей Закон підкреслює, що надання хмарних послуг повинно здійснюватися згідно з чинним законодавством, враховуючи вимоги «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні довірчі послуги», «Про захист персональних даних», «Про електронні комунікації», «Про Національний банк України», «Про державну таємницю», «Про доступ до публічної інформації» інших нормативно-правових актів України та міжнародних стандартів. При цьому захист інформації повинен здійснюватися відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах». Проте деякі питання щодо захисту державних даних залишаються відкритими, тож документ містить в собі білі плями для маніпуляцій, які повинні враховувати користувачі при підписанні договору про надання хмарних послуг між сторонами.

2.5.1 Умови використання хмарних послуг для роботи з інформацією з обмеженим доступом

Згідно із статтею 20 Закону України № 2657-XII «Про інформацію» [27], інформація поділяється на відкриту та з обмеженим доступом (далі - ІзОД). Детальна схема різновидів інформації за рівнем доступу зображена на рис. 11.

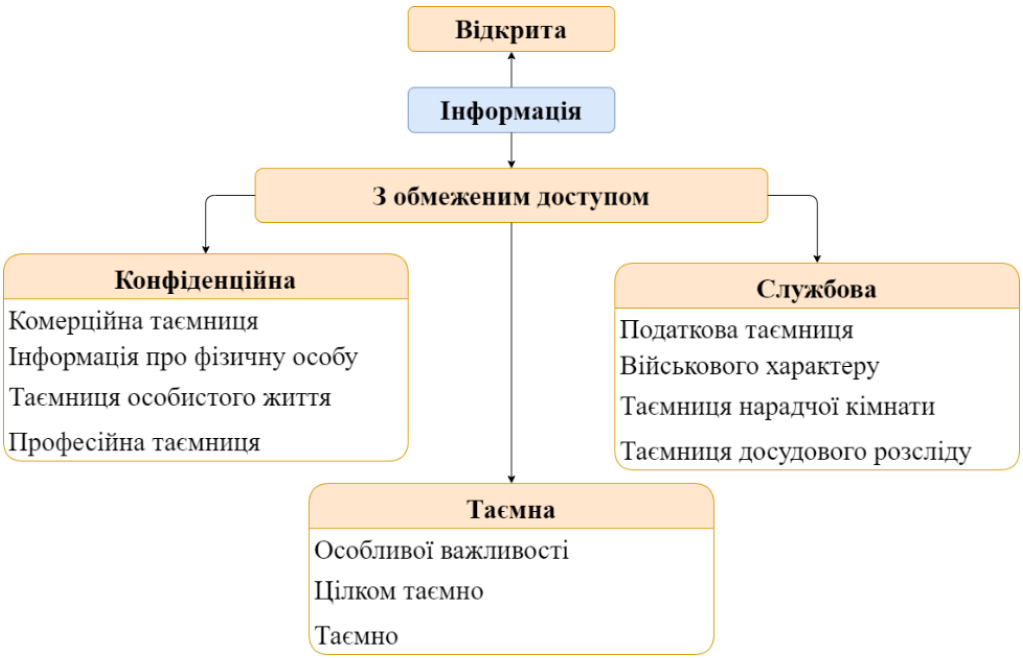

Рисунок 11 - Види інформації за рівнем доступу

До кожного із зазначених видів інформації застосовні особливі інструкції, які необхідні для забезпечення відповідного рівня безпеки, проте які значно ускладнюють, або навіть унеможливлюють використання хмарних технологій при роботі з ІзОД.

Наприклад, Закон України «Про державну таємницю» описує особливості поводження з інформацією різних ступенів секретності, від стадії віднесення даних до державної таємниці, етапів засекречення, налагодження захисту, спеціального порядку надання допуску, до процесу розсекречення і видалення. Охорона державної таємниці передбачає єдині вимоги до виготовлення, користування, збереження, передачі та обліку матеріальних носіїв секретної інформації, а також вимоги до технічного і криптографічного її захисту [28].

Таким чином, для кожної організації, яка планує провадити діяльність, що пов’язана з державною таємницею, пропонується дозвільний порядок за результатами спеціальної експертизи. Серед умов такої експертизи, поряд з наявністю спеціалізованих приміщень і техніки, є функціонування режимно-секретного органу, який контролює забезпечення секретності таємниці, що з перспективи надавача хмарних послуг є неможливим й не раціональним. Всі ці умови фактично унеможливлюють використання хмарних послуг при роботі з

інформацією, що належить що цієї категорії – суворий облік кожного з матеріальних носіїв секретної інформації здається малоймовірним в сучасних реаліях.

Основним нормативно-правовим актом, який регулює питання вимог до роботи із службовою інформацією є «Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», яку було затверджено постановою Кабінету Міністрів України у 2016 році [29]. Згідно з цією інструкцією, для передачі службової інформації забороняється використовувати відкриті канали зв'язку, а для обробки даних такого виду можна застосовувати лише ІТС, що відповідають вимогам законодавства у сфері захисту інформації і підлягають обліку за визначеною процедурою. Регламентовано також умови заміни електронних носіїв інформації – тільки в присутності власника цієї інформації.

2.5.2 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Як було вказано раніше, для правомірного здійснення своєї діяльності, надавач хмарних послуг зобов'язаний надати список документів, передбачений ст.8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [30]. Цей закон визначає умови обробки інформації в системі і передбачає необхідність підтвердження відповідності комплексної системи захисту інформації (далі – КСЗІ) за результатами спеціальної експертизи. Порядок проведення такої експертизи про задоволення вимог до засобів технічного і криптографічного захисту інформації визначений законодавством, а органи з оцінки відповідності (які керуються Законом України «Про технічні регламенти та оцінку відповідності») перед цим повинні пройти ретельну процедуру акредитації (яку здійснює, наприклад, Національне агентство з акредитації України).

Загальні вимоги забезпечення захисту державних інформресурсів затверджені постановою Кабінету Міністрів України «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних

системах». При цьому захисту в системі підлягають всі види інформації – відкрита (із забезпечення цілісності та доступності), конфіденційна, службова і таємна, а апаратно-програмні засоби захисту повинні мати не нижче третього рівня гарантій коректності надання послуг безпеки.

Особливі вимоги висуваються до апаратних, апаратно-програмних і програмних засобів криптографічного захисту інформації, які повинні відповідати порядку розробки, виробництва та експлуатації, мати спеціальну ліцензію від акредитованого органу відповідності після проведення випробувань. Звертається увага на особливості генерації ключових даних, порядку обліку, зберігання і знищення носіїв ключової інформації.

2.6 Стандарти з оцінки відповідності

Міжнародні нормативні документи сімейства ISO/IEC 17000 було прийнято як державні стандарти України для врегулювання процедури оцінки відповідності.

Згідно із Законом України «Про технічні регламенти та оцінку відповідності»: «оцінка відповідності – процес доведення того, що задані вимоги, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані» [31]. Проведенням цього процесу, а також калібруванням, випробуванням, сертифікацією та інспектуванням займається орган з оцінки відповідності.

ДСТУ ISO/IEC 17000:2020 описує функційний підхід як основний принцип оцінювання відповідності і представляє цей процес у вигляді послідовності трьох функцій: відбирання, визначання, критичний огляд і підтвердження відповідності. Такий підхід можна подати у вигляді схеми на рис. 12) [32].

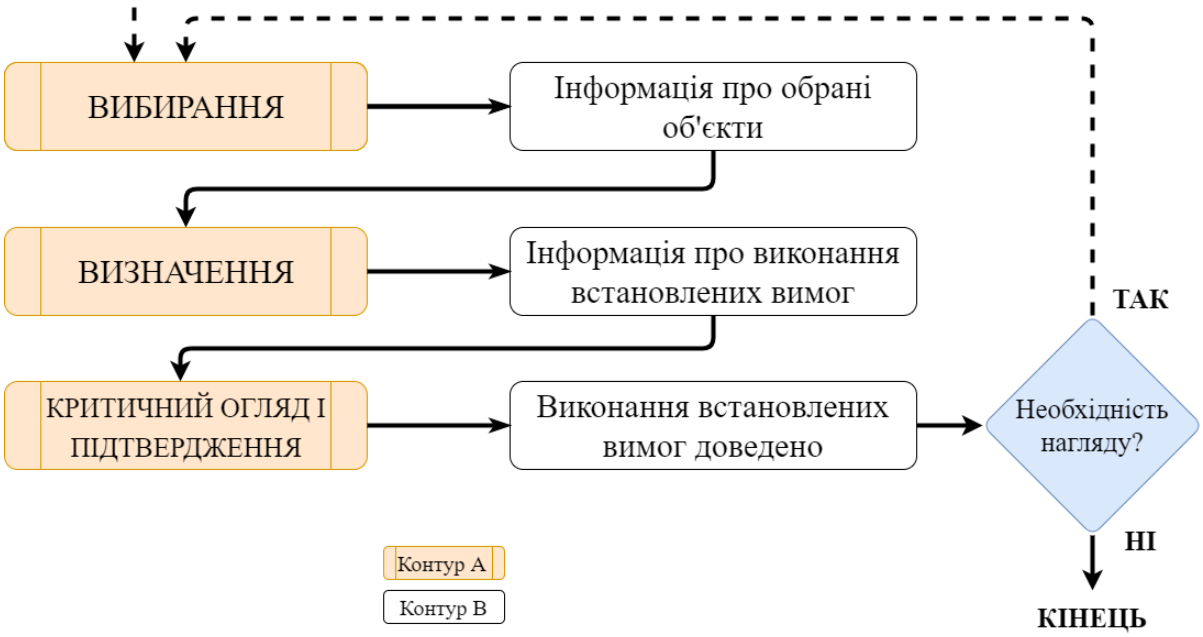

Рисунок 12 - Функційний підхід до оцінювання відповідності

Функція «Вибирання» враховує створення плану та підготовлення дій для збирання і подання інформації –об’єктом дослідження може стати все підприємство, КСЗІ загалом, або кожен його елемент. На цьому етапі відбираються найбільш придатні процедури оцінювання та необхідна додаткова інформація для доведення ефективного виконання необхідних вимог.

«Визначення» - встановлення, щоб подати всю інформацію про виконання вимог. Сюди ж можна віднести процедури випробування, інспектування, аудиту і рівноправного визначення.

«Критичний огляд» підтверджує правильність результатів перевірки і порівнює їх з усіма встановленими вимогами. Підсумком є рішення про відповідність обраних об’єктів.

«Необхідність нагляду» передбачає проведення процедури оцінки відповідності за потребою.

Загалом, діяльність щодо оцінювання відповідності можна характеризувати як діяльність «першої сторони» (тобто надавача послуг), «другої сторони» (користувача хмарних послуг) або «третьої сторони» (проведення оцінки уповноваженим органом).

Висновки за розділом 2

В даному розділі було розглянуто сукупність нормативних документів щодо технологій хмарних обчислень. Представлені у вигляді ієрархічної схеми залежно від рівня суб’єктів стандартизації або об'єкта регулювання, вони становлять базу для подальшої розробки процедур і схем оцінювання відповідності НХП представленим стандартам.

Зокрема, було проаналізовано міжнародні стандарти з безпеки хмарних технологій на прикладі документів ISO/IEC, досліджено різноманіття національних стандартів NIST, розглянуто структуру кібербезпеки, запропоновану цим інститутом, а також галузеві стандарти, які потрібно враховувати при користуванні хмарою у кожній сфері діяльності.

Окрім цього, в цьому розділі було здійснено детальний аналіз своєрідних ознак нормативно-правової бази України, що регламентують використання хмарних сервісів в державних та приватних установах та стандартизують процедуру проведення оцінки відповідності.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ З ОЦІНКИ ВІДПОВІДНОСТІ ВИМОГАМ НАДАВАЧІВ ХМАРНИХ ПОСЛУГ

3.1 Необхідність оцінки відповідності вимогам надавачів хмарних послуг

Оскільки технології хмарних обчислень стали глобальним трендом, хмарна відповідність вимогам є одним із ключових факторів при виборі провайдерів хмарних послуг та міграції користувачів у хмару.

Залежно від виду діяльності та рівня допустимого операційного ризику, користувачі хмарних послуг зобов'язані враховувати відповідність НХП щодо цілого комплексу законів і стандартів. Вони можуть мати схожі положення, але деякі особливості є визначальними для окремих галузевих стандартів, які вже згадувались в попередньому розділі. Наприклад, PCI DSS, який використовується для забезпечення безпеки платежів, має особливі вимоги до розгортання хмар. Те ж саме стосується HIPAA в галузі охорони здоров'я. Іншим прикладом є GDPR, який забороняє передачу особистої інформації за межі ЄС, що також ускладнює співпрацю з НХП.

Підхід, що базується на оцінці відповідності НХП вимогам стандартів, гарантує високий рівень впевненості клієнтів щодо безпеки інформаційної системи - механізми зберігання, передачі, відображення та архівування даних користувача є чітко визначеними. Більше того, відповідність хмарних систем вимогам міжнародних стандартів дозволяє користувачам використовувати послуги різних провайдерів, адже така оцінка може виступати індикатором їх сумісності.

Водночас, якщо постачальник використовує хмарний сервіс, який не відповідає вимогам, на компанію очікують значні штрафні санкції і, що найвагоміше, користувачі в такому випадку не зможуть бути впевненими в належному рівні інформаційної безпеки хмари, що може призвести до реальних кейсів із втрати або компрометації даних та значних репутаційних втрат.

Проте відповідність хмарним вимогам — це не лише відповідальність постачальників хмарних послуг. Так, НХП мають спеціальні сертифікати відповідності та звіти аудитів безпеки, які вони повинні пройти для забезпечення безпеки інформаційних систем, але саме організація-користувач хмарних послуг несе відповідальність за пошук правильного постачальника на основі вимог кібербезпеки бізнес-індустрії та залишається власником своїх даних, незважаючи на фізичну відсутність контролів безпеки у хмарі.

Більшість постачальників хмарних послуг несуть спільну відповідальність з користувачами, тобто розрізняють «безпеку хмари» (відповідальність постачальника хмарних послуг) та «безпеку в хмарі» (відповідальність користувача). Це означає, що постачальник обіцяє підтримувати безпеку інфраструктури та пропонує надійні інструменти безпеки, але відповідальність за налаштування та захист своїх даних, підтримання постійного регуляторного контролю лежить на клієнті і, в кінцевому підсумку, повна вага захисту інформації, лежить саме на користувачеві хмарних послуг. Постачальник хмарних послуг перелічує гарантії відповідності під час укладення SLA, але компанія має самостійно перевіряти постачальників і забезпечувати безпеку даних, переданих стороннім рішенням. Організаціям необхідно використовувати інструменти, запропоновані НХП, а також інші інструменти, щоб забезпечити повну видимість і керування всіма своїми мережевими засобами безпеки.

Компанії зазвичай розглядають SLA як прості шаблонні документи, наражаючи цим себе на додаткові ризики. Проте саме ці документи створюють додатковий договірний тиск на НХП, щоб вони дотримувалися правил та могли бути притягнуті до відповідальності за порушення умов угоди.

Надавач хмарних послуг, у свою чергу, після проведення оцінки відповідності вимогам безпеки отримує довіру клієнтів і можливість працювати над масштабнішими, більш прибутковими проектами, що вимагають високого рівня гарантій щодо впровадження надійної безпеки інформаційної системи і чутливих даних, що в ній оброблюються.

Оцінка відповідності стандартам безпеки може стати відправною точкою, щоб визначити свою політику інформаційної безпеки (далі - ПІБ) та боротися із загрозами, що притаманні хмарним сервісам. Фактично, оцінка відповідності передбачає проведення аудиту безпеки хмарної системи НХП згідно з стандартизованим набором вимог з метою отримання відповідного сертифікату для демонстрації гарантій безпеки потенційним клієнтам хмарних сервісів. Сукупність вимог, які встановлюють стандарти безпеки, ґрунтується на найкращих міжнародних практиках, тож це допомагає НХП врахувати всі необхідні аспекти безпеки інформаційної системи та вдосконалити її через усунення виявлених розривів між існуючими засобами контролю системи та тим, що необхідно для безпечної мережі.

При цьому проведення регулярних процедур оцінки відповідності допомагає отримати більш повне розуміння своїх онлайн-операцій та архітектури, перевірити, чи ефективно відбувається захист даних користувачів від усіх потенційних векторів і методів атак, допомагає оптимізувати необхідні ресурси, визначити потребу у навчанні співробітників, розробити плани аварійного відновлення і реагування на інциденти, а також визначити потенційні ризики безпеки і побудувати плани їх усунення [33].

3.2 Рекомендації щодо процедури проведення оцінки відповідності надавачів хмарних послуг

Загалом, функційний підхід, описаний ДСТУ ISO/IEC 17000:2020 (див. рис. 12) може бути застосовний для проведення оцінки відповідності надавачів хмарних послуг [32]. Проте для підвищення ефективності цієї процедури варто враховувати деякі нюанси, що стосуються більшою мірою ринку хмарних обчислень.

Деталізована та доповнена версія схематичного ображення функційного підходу до оцінки відповідності надавачів хмарних послуг зображена на рис. 13.

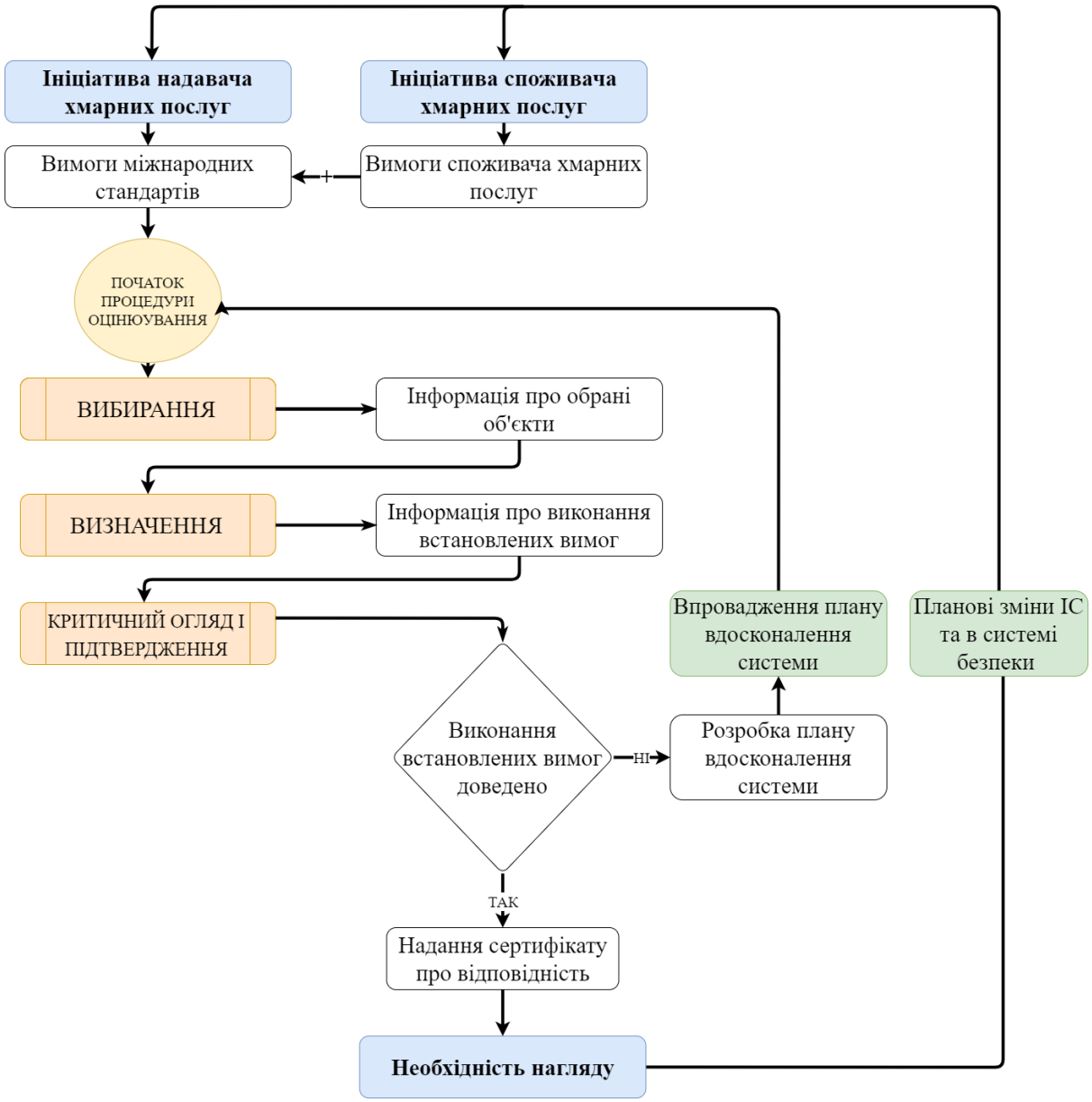

Рисунок 13 - Розширений функційний підхід до оцінювання відповідності надавачів хмарних послуг

Ключовою особливістю інформаційних технологій, порівняно з іншими галузями діяльності, є дуже висока динамічність розвитку, тому функція «Необхідність нагляду» стає критично важливою в цій сфері – надавачі хмарних послуг потребують систематичного проведення контролю безпеки ІС і підтвердження відповідності вимогам як міжнародних стандартів, нормативних актів, законодавства України так і контрактних умов.

Окрім цього, потрібно передбачити функцію «Вдосконалення системи», яка буде описувати зміни фізичної, логічної та організаційної структури організації для того щоб полегшити наступні процедури оцінки відповідності.

Схема також визначає два основних джерела ініціалізації проведення процедури оцінки відповідності – це може бути як ініціатива НХП, так і запит потенційних користувачів хмарних послуг, які визначили пакет стандартів, необхідних для ведення бізнесу та накладають власні вимоги до безпеки інформаційних систем.

Надання сертифікату про відповідність має свої особливості та потребує окремо визначених процедур управління. Головними умовами видачі сертифіката є успішна оцінка хмарного сервісу та перевірка результатів цієї оцінки, який має виконуватись незалежно і охоплювати огляд усіх наданих звітів, щоб переконатися в тому, що висновки узгоджуються з наданими доказами та правильно застосовано прийняті критерії та методи оцінки. Орган, відповідальний за сертифікацію НХП встановлює термін дії сертифіката, який не перевищує трьох років. Протягом цього терміну необхідні періодичні повторні оцінки, щоб гарантувати постійне виконання провайдером встановлених вимог. Відповідно до результатів оцінювання, сертифікат може набувати різних статусів. Наприклад, статус «Новий» (коли НХП вперше підтвердив свою відповідність), «Оновлений» (для відображення деяких змін), «Зупинений» (до виправлення невідповідностей), «Поновлений» (після підтвердження усунення виявлених недоліків), «Продовжений» (затверджений без змін після закінчення терміну дії), «Відкликаний» (через незадоволення вимог безпеки після трьох місяців від призупинення дії сертифікату).

3.3 Аналіз існуючих специфікацій

Існує декілька загальноприйнятих схем що містять загальний перелік вимог до НХП та методи проведення процедур їх сертифікації.

Зокрема, мінімальною вимогою при виборі постачальників хмарних послуг є відповідність стандарту Service Organization Control 2 (далі - SOC 2). Це процедура

аудиту, розроблена AICPA, яка гарантує, що постачальники послуг безпечно керують даними користувачів для захисту інтересів організації та конфіденційності її клієнтів. Звіт про аудит SOC 2 демонструє, що НХП дотримується політики, процедур та засобів контролю, які відповідають п’яти принципам довіри: безпека, доступність, цілісність обробки, конфіденційність та приватність.

Існує два типи звітів SOC:

- Тип I описує системи постачальника та чи відповідає їхня конструкція відповідним принципам довіри.
- Тип II детально описує експлуатаційну ефективність цих систем.

На відміну від PCI DSS , який має дуже жорсткі вимоги, звіти SOC 2 унікальні для кожної організації. Відповідно до певної ділової практики кожен розробляє власні засоби контролю, щоб відповідати принципам довіри [34].

Найбільш відомою схемою сертифікації є Cloud Controls Matrix (далі - CCM) розроблена Cloud Security Alliance (CSA). Місія цієї організації полягає в тому, щоб «сприяти використанню найкращих практик забезпечення безпеки в хмарних обчисленнях», саме CSA створила першу в галузі сертифікацію хмарної безпеки в 2010 році, яка наразі є загальновизнаною у світі [35].

CCM - це структура керування кібербезпекою для хмарних обчислень, яка відповідає найкращим практикам CSA та вважається фактичним стандартом хмарної безпеки й конфіденційності. Ця матриця контролів містить 16 доменів, які охоплюють усі ключові аспекти хмарних технологій. Кожен домен розбитий на 133 контрольні цілі. CCM служить керівництвом, щоб допомогти організаціям визначити спільні обов’язки між надавачем та користувачами хмарних послуг під час впровадження контролю безпеки. Для кожного елемента керування він також визначає, які хмарні архітектурні й організаційні моделі стека й хмарних сервісів застосовні.

Вимоги, вказані в CCM зіставляються з прийнятими міжнародними й галузевими стандартами безпеки, правилами та структурами контролю, а саме ISO/IEC 27001/27002/27017/27018, NIST 800-53, FedRamp, PCI DSS, AICPA TSC,

CIS Controls, ISACA COBIT, NERC CIP та державними стандартами BSI C5 (Німеччина) і SecNumCloud (Франція).

CCM використовується як стандарт для оцінки стану безпеки організацій у реєстрі The Security, Trust, Assurance, and Risk Registry (далі - STAR). STAR - це загальнодоступний реєстр, який документує засоби контролю безпеки та конфіденційності, що надаються популярними пропозиціями хмарних обчислень. STAR охоплює ключові принципи прозорості, суворого аудиту та відповідності стандартів, викладених у CCM. Публікація в реєстрі дозволяє організаціям продемонструвати поточним і потенційним клієнтам свою позицію щодо безпеки та відповідності, включаючи правила, стандарти та політики, яких вони дотримуються. При цьому STAR пропонує два рівня гарантій – перший рівень передбачає самостійну оцінку НХП, а другий – проведення аудиту третьої сторони.

Для спрощення проведення оцінки відповідності, CSA розробила супровідний Опитувальник ініціативи з оцінки консенсусу (CAIQ), який містить набір запитань «так чи ні» на основі засобів контролю безпеки в CCM.

Головною європейською схемою для оцінки відповідності НХП є Схема сертифікації кібербезпеки Європейського Союзу для хмарних послуг (далі - EUCS) [36].

Схема EUCS не є окремою схемою; це частина європейської системи сертифікації з кібербезпеки, яка може застосовуватися до всіх хмарних служб, дотримуючись деяких принципів:

- Схема EUCS розрізняє різні категорії хмарних послуг, спираючись на типи хмарних можливостей (інфраструктура, платформа, додаток);

- Схема EUCS спрямована на встановлення відповідності хмарних послуг набору вимог, що відповідають одному з рівнів гарантії, визначених у схемі EUCS;

- Схема EUCS має на меті зробити географічну та юридичну інформацію про хмарні послуги доступною та зрозумілою для всіх користувачів схеми, щоб дозволити використовувати їх у разі потреби.

- Схема EUCS визнає, що відповідальність за безпеку хмарної послуги розподілена між Постачальником і Замовником хмарних послуг, та спрямована на

перевірку того, що цей розподіл відповідальності чітко та публічно задокументовано.

- Схема EUCS спрямована на надання достатньої інформації для прийняття обґрунтованих рішень щодо безпеки щодо хмарних послуг потенційним клієнтам і клієнтам з достатніми знаннями з кібербезпеки, дозволяючи їм повністю зрозуміти та впровадити документацію, яка визначає їхню відповідальність.

Схема ґрунтується на багатьох різних джерелах, першим із яких є звіт робочої групи Cloud Service Provider Certification (далі - CSP-CERT), що був представлений у 2019 році та надав базову основу, на основі якої була розроблена EUCS, вимоги безпеки, визначені в схемі, значною мірою спираються на стандарти серії ISO27000, німецьку схему BSI C5, SecNumCloud, звіту CSP-CERT та з принципів інших схем, що використовуються в Європі, а процедура оцінки відповідності заснована на стандарті ISO/IEC 17065.

3.4 Рівні гарантій при оцінюванні відповідності вимогам безпеки

При проведенні оцінки відповідності вимогам варто враховувати неоднорідну структуру інформації, яка буде оброблятись та зберігатись в хмарних системах. Деяким користувачам важлива не стільки безпека даних, як висока продуктивність системи хмарних обчислень, тоді як для інших – систем, які працюють з конфіденційною інформацією, персональними даними та іншою чутливою інформацією, гарантія безпечності хмарних систем є критично необхідною. Саме тому сертифікація надавачів хмарних послуг повинна передбачати декілька рівнів гарантій, відповідно до потреб користувачів. Рівень гарантій повинен бути співмірним з рівнем ризику, пов’язаним з передбачуваним використанням продуктів, послуг або процесів, які пропонує хмарна система. Отож, вимоги безпеки, що відповідають кожному рівню гарантії, повинні бути задокументовані у відповідній схемі сертифікації інформаційної безпеки, включаючи відповідні функції безпеки та відповідну суворість і глибину оцінки, яку має пройти надавач хмарних послуг.

Оптимальним варіантом є розподіл вимог, запропонований EUCSA , який передбачає три рівні гарантій безпеки: «базовий», «середній» та «високий».

Базовий рівень гарантій призначений для мінімізації відомих основних ризиків інцидентів та кібератак і може бути додатково визначений наступним чином:

- забезпечує обмежену впевненість у тому, що хмарна служба створена та функціонує з процедурами та механізмами для відповідності вимогам безпеки на рівні, призначеному для мінімізації відомих основних ризиків інцидентів та кібератак.

- придатний для хмарних сервісів, які розроблені відповідно до типових вимог безпеки до служб для некритичних даних і систем.

- типовий профіль зловмисника – це особа з обмеженими навичками, що повторює відому атаку з обмеженими ресурсами, не маючи здатність виконувати атаки соціальної інженерії.

- глибина оцінки повинна складатися виключно з інспекційних заходів, заснованих на перевірці повноти та узгодженості наданої документації щодо процесів і проекту, призначених для підтвердження виконання технічних та організаційних заходів, включаючи вимоги до повністю автоматизованого тестування основних відомих вразливостей та автоматизованої перевірки відповідності за заздалегідь визначеним планом аудиту.

Середній рівень гарантій призначений для мінімізації відомих ризиків кібербезпеки, а також ризику інцидентів та кібератак, здійснених суб’єктами з обмеженими навичками та ресурсами, і може бути додатково визначений наступним чином:

- надає достатню впевненість, що хмарна служба створена та функціонує за допомогою процедур і механізмів для мінімізації відомих ризиків кібербезпеки, а також ризику інцидентів та кібератак, які здійснюються суб’єктами з обмеженими навичками та ресурсами. Постачальник хмарних послуг оцінив ці ризики та запровадив відповідні засоби контролю, які, якщо вони працюють ефективно, мінімізують ці ризики та відповідають відповідним вимогам безпеки протягом визначеного періоду.

- придатний для хмарних сервісів, які призначені для відповідності типовим вимогам безпеки до послуг для критично важливих для бізнесу даних і систем.

- типовим профілем зловмисника може бути невелика команда людей зі здібностями до хакерства та доступом до широкого спектру відомих методів злому, включаючи соціальну інженерію, але з обмеженими ресурсами, зокрема для здійснення широких атак або виявлення раніше невідомих вразливостей. .

- обсяг оцінки для рівня впевненості «Середній» повинен включати, на додаток до вимог до рівня впевненості «Базовий», аудит на місці, включаючи інтерв'ю та інспектування зразків, а також перевірку того, що впровадження відповідає зазначеним процесам та дизайну, включаючи валідацію функціонального випробування, проведені на цій реалізації. Контроль безпеки для рівня впевненості «Суттєвий» повинен включати обмежене тестування з використанням відомих атак.

Високий рівень гарантій призначений для мінімізації ризику сучасних кібератак, які здійснюються акторами зі значними навичками та ресурсами і може бути додатково визначений наступним чином:

- забезпечує високу впевненість, що хмарна служба створена та функціонує з використанням процедур і механізмів для мінімізації ризику сучасних кібератак, які здійснюються суб'єктами, які мають значні навички та ресурси. Постачальник хмарних послуг оцінив ці ризики та запровадив відповідні засоби контролю, які ефективно діяли, щоб мінімізувати ці ризики та відповідати відповідним вимогам безпеки протягом визначеного періоду.

- забезпечує автоматичний моніторинг безперервної роботи елементів керування відповідно до їхньої конструкції, а також засоби контролю, які повинні регулярно переглядатися та перевірятися ручкою для підтвердження їх фактичного здатність запобігати або виявляти порушення безпеки.

- підходить для хмарних сервісів, які розроблені, щоб задовольнити специфічні вимоги безпеки для критично важливих даних і систем.

- типовий профіль зловмисника для високого рівня впевненості має бути командою висококваліфікованих людей, які мають доступ до значних ресурсів для

розробки та здійснення атак, отримання доступу до інсайдерів, виявлення або придбання доступу до раніше невідомих вразливостей.

- глибина оцінки для рівня впевненості «Високий» повинна базуватися на глибині для рівня впевненості «Середній», до якої повинні бути додані вимоги щодо глибини інспектування або тестування, щоб перевірити, що засоби контролю, запроваджені надавачем хмарних послуг, дійсно відповідають своїй меті. Зокрема, ці вимоги стосуються автоматизованого моніторингу засобів контролю та огляду та тестування на проникнення засобів контролю безпеки. Такі дії плануються на кілька років, і вони повинні виконуватися персоналом з відповідними компетенціями, зокрема, коли необхідні випробування на проникнення або поглиблені технічні огляди.

Варто зазначити, що середній рівень гарантій враховує вимоги до базового рівня, встановлюючи додаткові умови, що можуть гарантувати більш високий рівень інформаційної безпеки, а високий рівень гарантій, у свою чергу, накладає власні додаткові вимоги до вже доповненого середнього рівня.

Запропоновані рівні гарантій передбачають розробку особливих вимог до забезпечення безпеки інформаційних систем надавачів хмарних послуг відповідно до класифікації критичності систем і даних потенційних споживачів хмарних послуг. В такому випадку, оцінка відповідності вимогам демонструє користувачам, наскільки високими є гарантії інформаційної безпеки при користуванні послугами надавачів хмари.

3.5 Рекомендовані вимоги до надавачів хмарних послуг

Керуючись нормативними актами, нормами міжнародних стандартів і вже розглянутими національними схемами з оцінювання кібербезпеки хмарних продуктів, сервісів і послуг [34; 35; 36], можна сформулювати узагальнений список вимог до безпеки надавачів хмарних послуг, який буде охоплювати всі необхідні умови та відповідати запропонованим рівням гарантій. Усі аспекти вимог безпеки слід розглядати з точки зору функціональних, фізичних та бізнес-вимог. Крім того,

вимоги безпеки повинні випливати з цілей безпеки та/або організаційних цілей і нормативних вимог.

Схеми, запропоновані в додатках А-Е, допомагають узагальнити контрольний список відповідності вимогам хмар, який допоможе визначити потенційні вузькі місця у хмарних системах. Для того щоб продемонструвати користувачу рівень хмарної інфраструктури, за який відповідає той чи інший контроль, визначити відповідальність за дотримання вимог згідно із впровадженими моделями послуг, а також забезпечити різні рівні гарантій, схеми містять відповідне розшарування. Так, ця схема може здатися складнішою для розуміння, ніж опитувальник від STAR або інші матриці контролю, на основі яких складався даний перелік вимог, проте поняття ІБ - це складна багатошарова компонента, яка вимагає різностороннього підходу і не допускає відповідей «Так» чи «Ні» в питаннях про наявність тих чи інших функцій. Кожні із вказаних в таблиці політик і процедур, які покликані забезпечити безпеку (і можуть гарантувати це користувачу хмарних сервісів) повинні бути донесені до відома усім зацікавленим особам для прийняття вирішального однозначного рішення про доцільність, правомірність і, що найголовніше, безпечність користування тим чи іншим рівнем послуг надавача хмарних послуг відповідно до вимог законодавства, національних стандартів і договірних умов, розуміючи та враховуючи всі наявні ризики для бізнесу і даних, які будуть оброблятися та зберігатися на стороні хмари і необхідні умови, кожна з яких відповідає запропонованим рівням гарантій.

3.5.1 Організація інформаційної безпеки

Оптимальний перелік вимог до СУІБ, глобальної ПІБ, а також з аудиту безпеки та відповідності стандартам, відповідно до рівня гарантій при оцінюванні відповідності НХП запропонований в Додатку А.

Організаційні засади захисту інформаційних технологій є базовим рівнем, який визначає всі подальші аспекти захисту кожного елемента технологій хмарних обчислень і є вагомим підґрунтям для розробки політики інформаційної безпеки

(ПІБ) організації і функціонування системи інформаційної безпеки надавача хмарних послуг. Нижче наведені основні компоненти організації інформаційної безпеки НХП.

1) Система управління інформаційною безпекою (далі - СУІБ).

Ключовим об’єктом організації інформаційної безпеки є система управління інформаційною безпекою, якою керує НХП. Сфера застосування СУІБ охоплює організаційні підрозділи системи, а також місця і процеси для надання хмарних послуг.

2) ПІБ.

Вагому роль в організації інформаційної безпеки відіграє ПІБ як набір правил, політик і процедур, призначених для забезпечення того, щоб усі кінцеві користувачі та мережі в організації відповідали мінімальним вимогам безпеки ІТ та захисту даних. Цей документ встановлює загальний підхід до інформаційної безпеки НХП та може стати визначальним фактором при оцінюванні безпечності хмарних сервісів.

3) Аудит з безпеки та відповідність стандартам.

Надавачі хмарних послуг повинні розробити налаштовану інтегровану структуру політик і процедур аудиту та надання гарантій якості послуг, а також проводити оцінку (зокрема, із залученням незалежних експертів) й оновлення цієї політики щонайменше один раз на рік.

Для ефективного оцінювання безпеки, така політика повинна визначати сукупний перелік основних вимог – юридичних (відповідно до національних законів), нормативних (наприклад, вимоги щодо захисту даних), самостійно визначених та договірних (ними можуть бути PSI-DSS, SOC2, HIIPA), що стосуються інформаційної безпеки.

Проведення аудиту та оцінки якості послуг повинно відбуватись відповідно до плану, який буде враховувати ризики бізнесу й безпеки хмарних обчислень. При цьому систематично потрібно перевіряти відповідність діючим стандартам, нормативним актам, юридичним/контрактним зобов’язанням і законодавству, застосовним до процедури аудиту.

Відповідно до висновків аудиту, надавачі хмарних послуг зобов’язані ухвалити план коригувальних дій, заснованих на оцінці ризиків і звітувати зацікавленим сторонам про стан відновлення якості своїх послуг.

3.5.2 Управління активами організації

Рекомендовані вимоги до управління активами та персоналом організації відповідно до рівня гарантій при оцінюванні відповідності НХП перераховані в Додатку Б.

Активи включають фізичні та віртуальні об’єкти, необхідні для інформаційної безпеки хмарного сервісу під час створення, обробки, зберігання, передачі, видалення або знищення інформації в зоні відповідальності НХП. До їх переліку входять, наприклад, брандмауери, балансувальники навантаження, веб-сервери додатків і сервери баз даних. Особливим активом організації вважаються також людські ресурси, як потребують особливої уваги, адже вони є критичним елементом інформаційної безпеки інформаційної системи.

1) Управління активами.

НХП повинен визначити власні активи організації і забезпечити належний рівень їх захисту протягом усього життєвого циклу. Він включає етапи затвердження придбання, введення в експлуатацію, виведення з експлуатації та утилізації обладнання. При цьому варто враховувати інвентаризацію та класифікацію активів, безпечного налаштування механізмів обробки помилок, реєстрації, шифрування, автентифікації та авторизації, обмеження використання ПЗ або використання сервісів, захист від шкідливих програм, віддалена дезактивація або блокування, фізична доставка і транспортування, робота з вразливостями та повне видалення даних після виведення з експлуатації.

2) Управління персоналом.

Навмисні та ненавмисні дії працівників залишаються найбільш розповсюдженим джерелом загроз витоку даних. Для уникнення ризиків, пов’язаних із інсайдерами організації, кожен з учасників відносин у сфері хмарних обчислень

повинен суворо дотримуватись правил для співробітників, встановлених політикою безпеки організації. Це положення організація включає в трудові договори, де додатково задокументовані умови, ролі та відповідальність працівників за їх порушення. Окрім цього, керівництво організації повинне визначати, документувати та переглядати через заплановані проміжки часу вимоги угоди про нерозголошення/конфіденційність, що відображають потреби організації щодо захисту даних та операційних деталей.

Обов'язковою є перевірка усіх нових співробітників, включно з штатними працівниками, віддаленими співробітниками, підрядниками і третіми сторонами. Ця процедура повинна виконуватись відкрито, відповідно до місцевих законів, правил, етики та контрактів обмежень і пропорційно критичності даних, до яких необхідно отримати доступ, вимогам бізнесу та прийнятному ризику відповідно до ролі та обов'язків працівників.

Політика управління персоналом повинна давати чіткі вказівки щодо користування активами організації – описувати очікувану та неприпустиму поведінку і організацію моніторингової діяльності. Працівники підписують трудову угоду перед тим, як отримати доступ до організаційних інформаційних систем, ресурсів та активів. Ці правила включають порядок користування інформаційними системами організації, а також власними пристроями обробки інформації, якщо компанія допускає таку можливість, впроваджуючи політику Bring Your Own Device (далі - BYOD). Вони не можуть залишати свої робочі місця без нагляду, повинні виконувати політику «чистого столу» і зобов'язані підтримувати політики та процедури для захисту інформації, до якої здійснюється доступ, що обробляється або зберігається на віддалених сайтах і місцях, щоб знизити ризик несанкціонованого доступу до інформації. Керівники також мають встановити процедури повернення майна організації (пристрої автоматизованих робочих місць, портативні пристрої, копії інформації та апаратного забезпечення автентифікації) після припинення дії контракту, знищення власних активів, звільнення приміщень за необхідності.

Організаціям, які допускають дистанційну роботу, слід видати політику, яка визначає умови та обмеження роботи поза звичайним офісом. Захищені комунікації в такому випадку повинні враховувати необхідність авторизованого віддаленого доступу до внутрішніх систем організації, запобігаючи обробці та зберіганню інформації на приватному обладнанні, забезпечуючи конфіденційність інформації при передачі по лінії зв'язку і передбачаючи можливість відкликання повноважень, прав доступу та повернення активів організації.

Усі співробітники повинні бути обізнані про їхню роль і відповідальність за дотримання встановлених політик і процедур, а також відповідних юридичних, законодавчих або нормативних зобов'язань. Керівництво може надати доступ до конфіденційних організаційних та персональних даних лише співробітникам з відповідним навчанням щодо безпеки та регулярним оновленням організаційних процедур, тренінгів, тестувань, що стосуються їхньої професійної функції.

3.5.3 Критичні елементи управління безпекою

Рекомендований перелік вимог до управління ризиками, змінами, ланцюгами поставок, безперервністю бізнесу, та забезпеченням сумісності і портативності хмари, відповідно до рівня гарантій при оцінюванні відповідності НХП запропонований в Додатку В.

Таким чином, до критичних елементів управління безпекою хмарних систем можна віднести наступні компоненти:

1) Управління ризиками.

Надавач хмарних послуг зобов'язаний створити офіційну, задокументовану та спонсоровану керівництвом програму управління ризиками підприємства (далі - ERM), яка включає політику та процедури для ідентифікації, оцінки, володіння, обробки та прийняття ризиків хмарної безпеки та конфіденційності.

Програма ERM повинна враховувати ризики, пов'язані з інформаційною безпекою та конфіденційністю даних у хмарі. Програма повинна включати елементи управління ризиками, такі як ідентифікація ризиків, оцінка ризиків, обробка ризиків

та звітність про ризики. Управління кожною бізнес-сферою має складатися з впровадження відповідних програм і процедур ERM.

Програма ERM також має містити офіційну заяву про схильність до ризику та може включати створення та ведення реєстру ризиків, який відображає ймовірність виникнення, потенційний вплив на бізнес, рівні ризику та пропоновані дії щодо пом'якшення для кожного ризику.

Ця програма має визначити та розподілити ролі, відповідальність і зобов'язання керівництва. Для документування цих особливостей можна застосувати діаграми RACI - відповідальні, підзвітні, консультовані та інформовані, щоб краще відображати взаємозв'язки між ролями і обов'язками працівників.

Для більш високого рівня впевненості слід враховувати конкретні технічні ризики, зокрема:

- ризики виходу з ладу механізмів розподілу ресурсів технічної інфраструктури (пам'яті, обчислювальних ресурсів, сховища, мережі), які спільно використовують клієнти;

- ризики, пов'язані з неповним або незахищеним стиранням даних, що зберігаються в областях пам'яті або сховища, спільного для клієнтів, зокрема під час перерозподілу пам'яті та областей зберігання.

При цьому керівництво має сприяти координації між організаційними структурами, відповідальними за різні аспекти хмарної безпеки та ризиків конфіденційності і переглядати програму, за необхідності, щоб усунути зміни ландшафту загроз та істотні зміни в організації.

2) Управління змінами

Ринок інформаційних технологій є надзвичайно динамічним, тому зміни – невід'ємна складова хмарних обчислень, що зумовлює додаткові ризики до безпеки функціонування хмарних систем. Саме тому надавачі хмарних послуг повинні дотримуватись процедур управління ризиками, пов'язаних зі змінами в активах організації, включаючи програми, системи, інфраструктуру, конфігурацію систем тощо, незалежно від того, управління активами здійснюється внутрішньо чи зовнішньо.

Усі зміни в активах організації, додатках, системному програмному забезпеченні та інфраструктурі інформаційних технологій (наприклад, апаратне забезпечення, операційні системи, комунікаційне обладнання, програмне забезпечення) та пов’язані з ними конфігурації мають підпадати під дію політики управління змінами, бути перевірені, оцінені і задокументовані. Потрібно обмежити можливість несанкціонованого додавання, видалення, оновлення та керування активами організації і запровадити заходи виявлення з проактивним сповіщенням на випадок змін, що відхиляються від встановленого базового рівня контролю. Коли відхилення виявлено, надавач послуг повинен дотримуватися політики та процедур управління інцидентами.

При цьому необхідно передбачити процедуру управління винятками, в тому числі при виникненні надзвичайних ситуацій і визначити процедуру для активного відкату змін до попередньо відомого задовільного стану у разі помилок або проблем безпеки.

3) Управління ланцюгами поставок

Характерною особливістю хмарних технологій є модель спільної відповідальності за безпеку (далі - SSRM) кожного з учасників хмарних сервісів, включаючи треті сторони – постачальників продуктів і послуг. Саме тому важливо детально задокументувати та впровадити процедури застосування цієї моделі по всьому ланцюгу поставок. SSRM має чітко описувати кожну конкретну послугу на основі моделі хмарного сервісу та особливостей її реалізації. Відповідно, кожна сторона в ланцюжку поставок повинна документувати, впроваджувати та керувати своїми обов’язками SSRM щодо своєї конкретної служби. Це включає підтримку постачальників, що залучені до IaaS, SaaS та спеціалізованих послуг, які використовуються користувачами і надавачами хмарних послуг. Політика SSRM дозволяє підтримувати інвентаризацію всіх зв’язків надавача хмарних послуг та розуміти обсяг обов’язків і своєї відповідальності за кожен визначений елемент системи відповідно до моделі хмарного сервісу.

Політика та процедури для контролю та моніторингу третіх сторін, чиї продукти чи послуги сприяють наданні хмарного сервісу, охоплюють вимоги щодо

оцінки ризиків, які виникають при закупівлі послуг третьої сторони, класифікації третіх осіб, вимоги до інформаційної безпеки для обробки, зберігання або передачі інформації третім сторонам, вимоги щодо роботи з вразливими місцями, інцидентами безпеки, несправностями, а також специфікації для укладення договірної угоди і моніторингу вимог, що в ній вказані.

Надавач хмарних послуг має визначити та запровадити процес проведення внутрішніх оцінок для підтвердження відповідності та ефективності стандартів, політик, процедур і діяльності третіх сторін принаймні раз на рік, а також проведення оцінки безпеки для всіх організацій-учасників хмарних відносин, які повинні підтвердити відповідність застосовним міжнародним і галузевим стандартам, вимогам контракту і законодавства.

Для полегшення контролю моніторингу, НХП повинен мати централізований довідник постачальників, який складається з назви компанії, які сприяють наданню хмарних послуг, місця обробки і зберігання даних, а також відповідальні контактні особи постачальників послуг.

Важливо задокументувати стратегії, які забезпечуватимуть мінімальне порушення бізнесу в разі припинення відносин з постачальниками. Стратегії виходу повинні бути узгоджені з оперативними планами безперервності бізнесу та включати аналіз потенційних витрат, впливу, ресурсів і термінів переходу до альтернативного постачальника.

4) Управління безперервністю бізнесу

Одна із найбільших переваг, які пропонуються користувачам хмарних обчислень є гарантія безперервності ведення бізнесу за будь-яких умов, тому від надавачів послуг вимагається визначити вплив збоїв хмарних систем для розробки стратегій управління безперервністю бізнесу та операційної стійкості.

Аналіз впливу на бізнес (BIA) повинен включати наступні компоненти:

- Ідентифікація критичних продуктів і послуг з притаманними їм ризиками;
- Імовірність та вплив кожного ризику;
- Тривалість часу відновлення (RTO) і точки відновлення (RPO);
- Схильність організації до ризику;

- Ролі, відповідальність, повноваження та очікувані компетенції;

- Визначення відповідних контрзаходів для запобігання, виявлення та реагування на виявлені ризики;

- Розрахункові внутрішні та зовнішні ресурси, необхідні для відновлення.

Такий підхід дозволяє продемонструвати користувачам можливі ризики при використанні хмарних сервісів через демонстрування порогових критеріїв доступного ризику і зменшити їх вплив на основі результатів випробувань можливостей операційної стійкості системи, адже система безперервності бізнесу перевіряється на регулярній основі.

План управління безперервністю бізнесу передбачає створення резервних копій даних, що зберігаються в хмарі, забезпечення їх конфіденційності, цілісності і доступності, а також перевірку відновлення даних із створеної резервної копії.

Окрім цього, хмара повинна підтримувати план реагування на катастрофи для відновлення після стихійних і техногенних катастроф. Особливо актуальною є небезпека громадських заворушень, які можуть включати незадоволених працівників/підрядників/замовників, терористичні атаки, біологічні атаки та військові агенти. Тому такий план повинен виконуватись через регулярні проміжки часу на основі BIA організації. Він має виконуватися як тренувальна вправа та включати щорічні прямі події з місцевою владою (наприклад, пожежними підрозділами, посадовими особами охорони здоров’я, відділами поліції, антитерористичними організаціями та групами по боротьбі з кіберзлочинністю). План аварійного відновлення зобов’язує хмарних провайдерів доповнювати критичне для бізнесу обладнання резервним обладнанням, розташованим на розумній мінімальній відстані відповідно до застосовних галузевих стандартів або в рамках угод про рівень обслуговування SLA.

5) Сумісність і портативність

Користувачі хмарних сервісів повинні мати можливість доступу до хмари через інші хмарні сервіси або інформаційні системи клієнтів, а також отримати збережені дані після закінчення договірних відносин та безпечно видалити їх з хмари НХП.

Для уникнення проблем із сумісністю, які можуть вникати в хмарі, надавачу хмарних послуг слід задокументувати вимоги до зв’язку між інтерфейсами програм, сумісні технології оброки інформації, портативність розробки додатків і обміну інформацією. Повинні бути впроваджені криптографічно безпечні та стандартизовані мережеві протоколи для керування, імпорту та експорту даних.

Провайдер повинен надати користувачу API, щоб вони програмно отримували свої дані для забезпечення взаємодії та переносимості. Вони покликані підтримувати взаємодію між компонентами та сприяти безпечній міграції додатків і даних між середовищами.

Угода з користувачем повинна включати положення, що визначають доступ користувачів хмарних технологій при розірванні договору, які будуть включати формат, обсяг даних, тривалість часу, протягом якого вони будуть зберігатися та політику видалення даних. Видалення даних користувачів також включає метадані, дані, що зберігаються в резервних копіях, а також технічні дані, що стосуються клієнта (наприклад, каталоги, сертифікати, конфігурації доступу).

Організація повинна використовувати тестування безпеки політики та процедур сумісності та портативності. Докази проведених і запланованих тестів безпеки для всіх систем сумісності та портативності повинні надаватися відповідно до контрактних угод або на запит користувачів.

3.5.4 Безпека хмарної інфраструктури та віртуального середовища

Рекомендований перелік вимог до фізичної безпеки хмарної інфраструктури, віртуального середовища, ЦОД, мережі, кінцевих точок, додатків та даних запропонований в Додатку Г.

Інфраструктура хмарних провайдерів викликає найбільшу недовіру у користувачів, адже відповідальність за її безпеку лежить тільки на надавачу хмарних послуг. Саме тому слід враховувати вимоги до процедур безпеки інфраструктури та віртуалізації. Для цього необхідно планувати та контролювати доступність, якість та достатню потужність ресурсів, оптимізувати їх розподіл, щоб забезпечити необхідну

продуктивність системи (для зменшення ризику перевантаження системи або простоїв через зниження попиту), здійснювати моніторинг, шифрування, а також обмеження зв'язку між розділеними, попередньо задокументованими виробничими та невиробничими середовищами будь-якого рівня ризику лише автентифікованими та авторизованими з'єднаннями, які визначаються потребами бізнесу.

Політика та процедури безпеки віртуалізації інфраструктури повинні включати, (але не обмежуються) наступними вимогами:

- керування та контроль життєвим циклом віртуальних машин (далі – ВМ);
- обмеження зберігання зображень і знімків ВМ;
- системи резервного копіювання та відновлення;
- додавання тегів для віртуальної машини на основі чутливості/рівня ризику;
- формалізований процес керування змінами для створення, зберігання та використання образів ВМ;
- узгоджена політика безпеки та конфігурація з фізичною мережею;
- впровадження технологій безпеки, які охоплюють фізичні та віртуальні середовища з послідовним керуванням політикою та системою забезпечення виконання;
- брандмауери, фізичні чи віртуальні, для ізоляції груп віртуальних машин від інших розміщених груп;
- проектування та впровадження доступу з кожного рівня довіри до фізичних та віртуальних систем управління та безпеки.

Усі фізичні та логічні компоненти системи, гіпервізори, робочі навантаження, хости та мережі (фізичні, віртуальні), транспортний потік між різними компонентами, канали зв'язку, зони безпеки, робочі навантаження на кожному хості, рівні безпеки для робочих навантажень, а також ролі та відповідальності за їх дотримання повинні бути задокументовані. Надавач хмарних послуг несе відповідальність за закріплення хоста, гостьової операційної системи, гіпервізора та

рівня управління інфраструктурою відповідно до міжнародних практик і за підтримки технічного контролю, як частину базової лінії безпеки.

Надавачам хмарних послуг рекомендовано впроваджувати захист від зловмисного програмного забезпечення, моніторинг цілісності файлів і журналювання, а також використовувати довіру на основі апаратного забезпечення до модулів віртуальної надійної платформи (vTPM). За можливості, організації повинні використовувати мінімалістичні, специфічні для контейнера операційні системи (далі - ОС) з вимкненими всіма іншими службами та функціональними можливостями, а також із файловими системами лише для читання та іншими методами посилення, які використовуються для зменшення поверхонь атак:

- хости, які запускають контейнери, повинні запускати лише контейнери, а не інші програми, такі як веб-сервери або бази даних, поза контейнерами;

- хости, які запускають контейнери, повинні постійно перевірятися на наявність вразливостей і швидко оновлюватися;

- основна ос не повинна запускати непотрібні системні служби;

- доступ до хоста контейнера має базуватися на принципах необхідності знати та найменших привілеїв;

- для контейнерів слід використовувати моніторинг цілісності файлів і виявлення вторгнень на хост.

Однією з найважливіших вимог є безпечне проектування, розробка, розгортання та налаштування додатків та інфраструктури таким чином, щоб доступ користувачів та доступ всередині організації був належно сегментований та відокремлений, контрольований та обмежений від інших орендарів. Можливі визначення сегментації мають варіюватися від «повної ізоляції» до «часткового логічного поділу критично важливих для бізнесу активів та/або персональних даних/конфіденційних даних користувача та сеансів». Робочі навантаження між орендарями та бізнес-напрямками мають бути сегментовані відповідно до концепції найменших привілеїв, щоб зменшити поверхню атаки. Крім того, для робочих навантажень слід використовувати теги робочого навантаження, імена ресурсів та ідентифікацію.

Окрім цього повинні використовуватись безпечні та зашифровані канали зв’язку під час міграції серверів, служб, додатків або даних у хмарні середовища. Такі канали повинні включати лише сучасні та затверджені протоколи. Безпечний зв’язок під час міграції фізичних серверів, служб, програм або даних у віртуалізоване середовище може використовувати комбінацію вимог до конфіденційності, цілісності, автентифікації джерела, авторизації та невідмовності.

Побудова захищеного каналу передачі інформації може бути реалізована на різних рівнях мережі. Слід використовувати безпечні канали передачі інформації (порти та протокол), такі як: SSL, SSH, TLS (на рівні програми), IPsec, ICMP (на мережевому рівні), та PPTP, ARP (які знаходяться на рівні посилання). Для цих протоколів слід використовувати лише сучасні версії (застарілі версії використовувати не можна). Крім того, слід використовувати лише захищений порт (наприклад, 443). Ці конфігурації потребують перегляду щонайменше раз на рік та підкріплення їх документованим обґрунтуванням усіх дозволених служб, протоколів, портів та компенсаційних елементів керування.

Вразливості у фізичному середовищі також несуть небезпеку у віртуальному середовищі. Недоліки конфігурації та недоліки в програмах, брандмауерах або мережах залишаються вразливими до експлойтів, спуфінгу, атак з відмови доступу (далі - DoS) тощо, тому методи глибокого захисту повинні використовуватися як для фізичного, так і для логічного та адміністративного управління.

1) Безпека ЦОД.

Фізичний захист інфраструктури може здатись трюїстичним, проте залишається одним із критично важливих в тому числі й для технологій хмарних обчислень.

Будь-які фізичні та логічні активи повинні бути класифіковані, каталогізовані та відстежувані на основі організаційного бізнес-ризику. Персонал ЦОД повинен використовувати рішення, яке дає змогу відстежувати інвентаризацію та керувати фізичним розташуванням серверів та інших активів ЦОД, виключаючи паперові та ручні процеси. Розміщене рішення для відстеження активів для серверів, комутаторів, відстеження активів ЦОД зазвичай використовує технології пасивної

радіочастотної ідентифікації, глобальної системи позиціонування та/або технології Bluetooth Low Energy.

Від надавачів хмарних послуг вимагається підтримувати політику та процедури для безпечної утилізації обладнання, яке використовується за межами приміщення організації. Якщо обладнання фізично не утилізовано, а клієнт вирішив відмовитись від послуг хмари, має бути передбачена процедура знищення, яка унеможливлює відновлення інформації. Крім того, клієнт може запитати підтвердження того, що дані були ефективно видалені.

Також потрібно дотримуватись процедур переміщення або передачі апаратного, програмного забезпечення, або даних в інше місце - запит на транспортування вимагає письмової або криптографічної перевірки авторизації, а зв'язок між службами, які полегшують переміщення робочих навантажень, даних додатків тощо, мають бути зашифровані на основі глобально визнаних криптоалгоритмів, таких як AES-256. Крім того, цей процес може включати такі заходи, як обфускація або деідентифікація для приховання персональної інформації, яка транспортується.

Власники об'єктів повинні прийняти стандарт ISO/IEC 27001. Необхідно запровадити фізичні периметри безпеки для захисту персоналу, даних, та інформаційних систем, встановити фізичні периметри безпеки між адміністративними та діловими зонами та зонами зберігання та обробки даних. Доступ до кожної із зон повинен бути доступним лише авторизованому персоналу, а входи і виходи - контролюватись за допомогою механізмів контролю фізичного доступу.. Організації повинні зберігати журнали доступу для уповноваженого персоналу не менше шести місяців.

Для безпеки ЦОД потрібно виконувати процедури та технічні заходи, які забезпечують захист силових та телекомунікаційних кабелів на основі ризиків від загрози перехоплення на всіх об'єктах (допускається електромагнітне екранування, відповідно до ISO/IEC 27002), підтримувати системи контролю навколишнього середовища в центрі обробки даних, які контролюють, підтримують та перевіряють умови температури та вологості відповідно до прийнятих галузевих стандартів,

відстежувати й тестувати послуги комунальних служб на безперервну роботу і зберігати критично важливе для бізнесу обладнання подалі від місць, які мають високу ймовірність екологічних катастроф або військових дій.

НХП повинен забезпечити захист інформації в мережах за допомогою спеціальних технічних засобів для виявлення та реагування на мережеві атаки, а також організаційних заходів. Зокрема, потрібно задокументувати вимоги до логічного і фізичного розподілення мережі на зони безпеки, дозволені комунікаційні відносини, мережеві та прикладні протоколи, особливості адміністративних мереж та міжмережне спілкування. Для здійснення моніторингу відповідності цим вимогам обов'язковим є регулярне оновлення топологічних схем мережі та переліку використовуваного мережевого обладнання.

2) Управління безпекою кінцевих точок.

Кінцеві точки – одне з найбільш вразливих місць інформаційної системи. Технології хмарної інфраструктури не є винятком. Надавач хмарних послуг повинен підтримувати політику безпечного користування кінцевими точками.

Політики та процедури для керованих і некерованих кінцевих точок (включаючи BYOD) мають включати список усіх кінцевих точок, перелік схвалених служб, додатків, розширень програм і плагінів, прийнятних для використання кінцевими точками під час доступу або зберігання даних, керованих організацією. Також ця політика визначає процес перевірки сумісності кінцевого пристрою з операційними системами та програмами, забороняє обхід інтегрованих засобів контролю безпеки на кінцевих точках (наприклад, джейлбрейк або рутинг) і передбачає процедури, пов'язані із втратою даних, які не належать компанії, якщо потрібне повне або часткове очищення пристрою.

Підтримується інвентаризація всіх кінцевих точок, які використовуються для зберігання та доступу до даних компанії, управління змінами в ОС та додатках на кінцевих точках, визначення правильної конфігурації, захист інформації від несанкціонованого розкриття на керованих кінцевих пристроях за допомогою шифрування (окремих файлів, даних або цілого пристрою) та застосування технологій запобігання ШПЗ. Кінцеві точки мають бути захищені за допомогою

правильно налаштованих брандмауерів для перевірки трафіку і технологій та правил запобігання витоку даних (DLP). Також повинна бути передбачена можливість віддалено видаляти дані компанії і вмикати геотрекінг для всіх керованих мобільних кінцевих точок.

Там, де це можливо, організації також повинні вимкнути порти, заборонити використання записувальних пристроїв, перевіряти змінні носії, вкладені файли електронної пошти та веб-трафік.

Процеси, процедури та технічні та/або договірні заходи для підтримки належної безпеки кінцевих точок третіх сторін з доступом до організаційних активів мають бути визначені і задокументовані надавачем хмарних послуг. Для некерованих кінцевих точок слід надавати рекомендації, виходячи з оцінкою ризику, прийнятного для системного доступу і зберігання інформації. Вони можуть включати використання технології контейнерів для ізоляції конфіденційних даних. Наприклад, організація, яка забороняє використовувати електронну пошту для конфіденційної інформації, може визначити, що доступ до електронної пошти компанії за допомогою особистого пристрою вимагає лише обмеженого контролю (наприклад, прийнятного пароля, екрана блокування, достатньо сучасного програмного забезпечення, і відсутність обходу контролю безпеки постачальника).

Письмові угоди повинні включати підтвердження того, що третя сторона несе відповідальність за безпеку даних, якими володіє третя сторона або іншим чином зберігає, обробляє чи передає від імені організації.

3) Безпека хмарних додатків.

Надавачі послуг зобов’язані ухвалити та підтримувати політики та процедури безпеки додатків для відповідного планування і організації можливостей безпеки хмарних сервісів відповідно до встановлених політик безпеки і галузевих стандартів.

Така політика повинна визначати ролі та обов’язки відповідальних працівників, встановлювати базові й унікальні вимоги до безпеки додатків (наприклад, проведення тестів NIST, ISO, OWASP та CIS), оцінки бізнес- і

технологічних ризиків, їх постійного автоматизованого моніторингу та вдосконалення.

Хмарні провайдери повинні сприяти використанню встановленого життєвого циклу розробки програмного забезпечення, щоб гарантувати, що безпека інтегрована в продукт з моменту його створення, а існуючі ризики були усунені на початкових етапах розробки. Це включає проектування, перегляд коду, дизайну, навчання безпечному кодуванню, стратегії тестування (функціонального, регресійного, безпекового тощо), тестування вразливостей, безпечного розгортання, управління змінами та процесами завершення існування додатку.

Прикладами технічних показників при проведенні тестування можуть бути підрахунок вразливостей за слабкими місцями/серйозністю/джерелами виявлення (огляд дизайну, огляд коду, статичне і динамічне тестування безпеки, тестування на проникнення або пошук вразливостей), середній час вирішення проблеми або підрахунок перевищення цілей рівня послуг з відновлення.

Ці задокументовані принципи повинні стосуватись не тільки додатків, що були створені власними силами, а й від зовнішніх постачальників.

4) Безпека даних.

Політика та процедури для класифікації, захисту й обробки даних протягом усього їхнього життєвого циклу є необхідною вимогою відповідно до всіх застосовних законів і правил, стандартів.

Політика безпеки даних повинна передбачати надійні методи для безпечного видалення даних без можливості їх відновлення, сувору інвентаризацію даних та їх потоків, щоб визначити власників інформації та їх обов’язки, які дані обробляються, де фізично зберігаються та обробляються, де знаходяться резервні копії і куди вони передаються.

Дані класифікуються, використовуючи поля класифікації даних, тегів або метаданих на основі стандартних платформ відповідно до їх типу та рівня чутливості, згідно з яким визначається матриця доступу для їх читання і модифікації.

Особливо важливо виконання цих вимог для роботи з ІзОД. Захист даних і конфіденційність мають бути включені за замовчуванням на етапі проектування та протягом життєвого циклу розробки продукту. Крім того, проектна документація повинна чітко описувати, як захищаються дані. Надавач хмарних послуг повинен забезпечити виконання необхідних заходів для захисту обробки, передачі й зберігання конфіденційної інформації та персональних даних, враховуючи передачу як зовні, так і всередині організації.

При цьому потрібно враховувати можливу процедуру передачі чутливої інформації до правоохоронних органів за запитом при проведенні розслідування і зробити цю процедуру прозорою для користувачів.

3.5.5 Управління ідентифікацією та доступом

Узагальнені ключові вимоги до організації управління ідентифікацією та доступом відповідно до рівня оцінювання представлені в Додатку Ґ.

Надавачі хмарних послуг повинні підтримувати політику та процедури для управління ідентифікацією та доступом до інформації та засобів обробки інформації. Вона включає в себе контроль доступу до реєстрації, керування та видалення цифрових ідентифікаційних даних, надійний парольний захист, інформацію про системні унікальні ідентифікатори і рівні доступу, застосовуючи політику контролю доступу на основі ролей та розподілу обов’язків.

Політики і процедури щодо ролей і прав доступу стосуються управління обліковими записами (далі - ОЗ) користувачів (від призначення унікальних ідентифікаторів, до блокування і відкликання ОЗ в разі бездіяльності або потенційної компрометації облікових даних) і управління правами доступу (їх надання, своєчасного оновлення або відкликання для уникнення можливості зловживань). При цьому процедури управління правами доступу мають застосовуватись динамічно, тобто зміни мають набирати чинності без потреби перезавантаження системи (якщо не було надано нових прав доступу, які вимагають більш суворого методу автентифікації).

Політика контролю доступу повинна містити інструкції щодо розподілу між технічною інфраструктурою інформаційної системи, яка надає хмарні послуги, обладнанням, необхідним для адміністрування хмарної служби і активів, які вона розміщує, та іншими інформаційними системами, а також підтримувати розподіл обов'язків між середовищем виробництва, тестування та розробки, обмежуючи доступ читання/запису до всіх середовищ і вимагаючи багаторівневого схвалення. Це не виключає взаємодію між наданням хмарного сервісу та іншими інформаційними системами, наприклад, для цілей виставлення рахунків або резервного копіювання, але для таких цілей мають бути чітко визначені інтерфейси.

Доступ до облікового запису користувача та сервісів має використовувати методи контролю доступу, такі як контроль доступу на основі ролей і контроль доступу на основі атрибутів. Організації слід дотримуватись принципу найменших привілеїв і принципу необхідності знати при впроваджені доступу до інформаційної системи і запровадити процес надання доступу користувачам, який авторизує, записує та повідомляє про зміни доступу до даних та активів. Крім того, повинні регулярно проводитись перевірки процесів доступу (включаючи аудит, якщо це необхідно), щоб визначити недотримання виконання цих принципів у найкоротший проміжок часу.

Організаціям слід підтримувати базу даних усіх системних ідентифікаторів, які мають доступ до різних хмарних середовищ та активів. База даних повинна ілюструвати кореляцію між цифровими ідентифікаторами, активами, де надається доступ, і типом доступу, який надається (тобто, бізнес-користувачі, система користувачі, користувачі з привілеями тощо). Крім того, базу даних слід регулярно переглядати, щоб переконатися, що доступ до всіх служб відкликається або змінюється на основі зміни посадових обов'язків.

Користувачі, які мають ОЗ з привілейованими правами доступу вимагають особливого контролю, тому варто передбачити процеси, процедури та технічні заходи для поділу ролей привілейованого доступу на обмежений період часу, щоб адміністративний доступ до даних, можливості шифрування та керування ключами і можливості ведення журналів були чіткими та розділеними.

НХП повинен також впровадити процедури та технічні заходи для багатофакторної автентифікації та політики єдиного входу (далі - SSO). Для доступу до всіх середовищ, включаючи невиробничі, потрібна надійна автентифікація (для персоналу це багатофакторна автентифікація, а для користувачів, які не є людьми – автентифікація за допомогою криптографічного механізму, який задовольняє вимоги безпеки).

Нарешті, весь доступ (особливо привілейований) слід реєструвати та відстежувати на предмет аномалій та несанкціонованого використання, а також пов’язувати з системами оповіщення відповідно до потреб за допомогою рішення для керування інформацією та подіями безпеки (далі - SIEM).

3.5.6 Криптографія та управління ключами

Трирівневий перелік узагальнених вимог до криптографічного захисту даних та управління ключами розглянуто в Додатку Д.

Криптографічна система захисту інформації - обов’язкова вимога до хмарних сервісів відповідно до законодавства України. Надавач хмарних послуг забезпечує криптографічний захист даних у стані спокою, які включають бази даних, робочі станції кінцевих користувачів і файлові сервери та в стані передачі (включає системні інтерфейси, загальнодоступні мережі та електронні повідомлення), із врахуванням класифікації даних та пов’язані ризики, використовуючи криптографічні бібліотеки та генератори випадкових чисел, сертифіковані за затвердженим стандартом.

Криптографія забезпечує захист даних: конфіденційність, цілісність, доступність та автентифікацію джерела. До того ж організації повинні мати можливість або шифрувати всю інформацію на пристроях зберігання (тобто повне шифрування диска), або шифрувати конкретні структури даних (наприклад, файли, записи чи поля).

Правила політики безпеки системи керування криптографічними ключами – також необхідна умова до надавачів хмарних послуг. Вони повинні захищати

конфіденційність, цілісність, доступність та автентифікацію джерела всіх ключів, алгоритмів і метаданих. Важливою вимогою до хмарних сервісів є забезпечення процедур, що стосуються ключового управління в хмарних системах: криптографічно захищена генерація ключів, безпечне розповсюдження приватних і секретних ключів, встановлення криптоперіодів, відкликання скомпрометованих ключів, знищення ключа, активація ключа, дезактивація ключа, керування інвентаризацією ключів і сертифікатів, зберігання та відновлення заархівованої ключової інформації, відновлення ключа, моніторингу ключових змін, перевірка цілісності збереженої ключової інформації перед її використанням, дезактивації, відкликання та знищення цих ключів після закінчення терміну дії або компрометації (включно з відкликанням ключів, які зберігаються в апаратних модулях безпеки.

Ефективність цих процесів та їх відповідність нормативним стандартом оцінюється під час проведення аудитів, конфіденційна інформація та інструменти яких мають бути також захищеними. Для всіх ключових змін, пов’язаних з управлінням, слід розраховувати аналіз витрат і рентабельності інвестицій. Кожен аналіз повинен повністю враховувати наступні наслідки запропонованих змін, включаючи залишкові ризики.

Можливість управляти ключами може бути надана для користувачів хмарних сервісів, проте обсяг ключів, їх довжина, алгоритми шифрування і відповідальність за керування політикою, процедурами і процесами повинні бути суворо задокументовані.

3.5.7 Операційна безпека

Перелік вимог, які були запропоновані для забезпечення управління загрозами та вразливостями, логування та моніторингу інцидентів безпеки, а також їх розслідування, відповідно до запропонованого рівня гарантій при оцінюванні відповідності НХП представлений в Додатку Е.

Операційна безпека системи забезпечує належну та регулярну роботу, включаючи відповідні заходи щодо планування та моніторингу потужностей

хмарних сервісів, захисту від шкідливих програм, процесів логування та моніторингу, а також боротьби з вразливими місцями інформаційної системи, загрозами безпеки та розслідуванням виявлених інцидентів. Зокрема, до операційної безпеки можна включити наступні аспекти:

1) Управління загрозами та вразливостями.

Щоб захистити системи хмарних обчислень від експлуатації вразливостей зловмисником, необхідно запровадити політику управління загрозами та вразливостями (далі - TVM) та процедури для виявлення, звітування та визначення пріоритетів усунення вразливостей, процедури для захисту від зловмисного програмного забезпечення на керованих активах, а також процедури та технічні заходи для забезпечення можливості як планового, так і екстреного реагування на вразливості на основі виявленого ризику. Потрібно передбачити регулярне оновлення засобів виявлення загроз на основі сигнатур та індикаторів компрометації – щотижня, або навіть частіше.

Політика TVM передбачає визначення активів, які входять до сфери застосування цієї політики, звертаючи увагу на необхідність дотримання чинного законодавства, міжнародних стандартів і договірних умов, частоту оцінок, методи оцінювання вразливостей, повідомлення про значні прогалини в безпеці системи, і можливості нейтралізації виявлених ризиків. Також політика TVM включає чітко визначений процес реагування на інциденти, що відповідає ризику організації та прийнятні періоди усунення загроз у порядку критичності обчислювальної інфраструктури. При цьому вразливості слід розставити в пріоритеті з точки зору їх відносного ризику, важливості, організаційного впливу та терміновості (за CVSS).

Рекомендується виконувати тестування на проникнення незалежними третіми сторонами для визначення рівня захищеності інформаційної системи та ефективного визначення пріоритетів усунення виявлених слабких сторін.

Політика захисту від шкідливих програм має бути зосереджена на перевірці як вхідного, так і вихідного трафіку та впровадженні засобів контролю для виявлення, запобігання, блокування та видалення зловмисного програмного забезпечення. Захист від зловмисного програмного забезпечення має бути інтегрований у всю

обчислювальну інфраструктуру, включаючи обчислення, мережу, кінцеві точки та захищені шлюзи доступу, а організації повинні централізовано керувати механізмами захисту від зловмисного програмного забезпечення, включаючи планування, впровадження, оцінку, авторизацію та моніторинг визначених організаційною системою контролю безпеки зловмисного програмного забезпечення. Цей процес допоможе злагоджено боротися зі зловмисним програмним забезпеченням протягом заздалегідь визначених термінів за допомогою відповідних інструментів, щоб забезпечити стійкість до ризиків.

Повинна бути впроваджена інтегрована система TVM, яка зможе вести облік загроз та вразливостей, виявлених з часом, та результатів дій щодо їх пом’якшення. Інтегровану систему TVM слід використовувати для пом’якшення всіх майбутніх ризиків, використовуючи попередній досвід заходів із пом’якшення, а також для складення графіку усунення виявлених вразливостей, його моніторингу і нагляду за залишковими ризиками.

2) Логування та моніторинг.

Організації, що використовують технології хмарних обчислень повинні відстежувати події, пов’язані з безпекою, у додатках та базовій інфраструктурі й впровадити систему для генерування сповіщень відповідальним зацікавленим сторонам на основі таких подій та відповідних показників.

Процедури логування і моніторингу повинні включати відомості щодо мети, обсягу, ролей, відповідальності працівників, інформацію про те, як обробляються інциденти безпеки, порогові значення, пріоритетний моніторинг відповідно до категорії ризиків, яку інформацію слід реєструвати і як довго її відстежувати. До журналу безпеки потрібно записувати інформацію про тип, час, місце, джерело та результати події, а також перелік осіб, які з нею пов’язані для подальшого проведення розслідування інциденту і розробки заходів реагування.

Доступ до журналів аудиту функціонування ІС та фізичного доступу осіб до ресурсів організації має бути обмежений, доступний тільки авторизованому персоналу із веденням записів, які забезпечують унікальний доступ до звітності.

Крім цього такі записи повинні бути захищені від несанкціонованої зміни чи видалення.

Постійний моніторинг журналів аудиту безпеки за визначеними процедурами є обов'язковим, щоб виявити підозрілу діяльність, яка не відповідає типовим або очікуваним шаблонам і вжити своєчасних дій щодо виявлених аномалій. До таких подій можна віднести індивідуальний доступ до об'єкта, дії, здійснені з адміністративними привілеями, недійсні спроби доступу, зміни механізмів ідентифікації (включаючи підвищення привілеїв), зупинка діяльності журналів аудиту, видалення або зміну даних. Таким чином, організації повинні впровадити процес своєчасного виявлення та звітування про збої критичних систем контролю безпеки за допомогою брандмауерів, систем виявлення вторгнень, систем запобігання вторгненням, моніторингу цілісності файлів, антивірусів, здійснення фізичного та механічного контролю доступу та механізмів реєстрації аудиту.

3) Розслідування інцидентів.

Після виявлення аномальної діяльності в системі, необхідно відреагувати на інцидент належним чином. За це відповідають заздалегідь визначені процедури управління інцидентами безпеки. Вони допомагають реалізувати коригуючі та превентивні дії, розслідувати інциденти, усувати їх наслідки, а також причини, що в подальшому вдосконалити систему захисту. Відповідні стандарти та процедури звітності повинні включати отримані уроки та ключові показники ефективності, які мають бути визначені та запроваджені для процесів реагування на інциденти та навчання.

Надавач хмарних послуг зобов'язаний розробити план реагування на інциденти, який утворює так звану дорожню карту для обробки інцидентів, пов'язаних із хмарними сервісами організації та продуктами та послугами, на які ці послуги покладаються. Ці плани мають застосовуватися незалежно від того, чи є ці залежності внутрішніми (наприклад, IT, операції, підтримка та юридичні) чи зовнішніми (постачальники, партнери, клієнти та інші треті сторони). План повинен бути надійним, своєчасним, узгодженим з планами організації безперервної

діяльності та аварійного відновлення, тому потребує регулярного тестування та оновлення.

Організаціям слід визначати, впроваджувати та контролювати показники, пов'язані з подіями та інцидентами, щоб виявити будь-які недоліки в операційних процесах або технічних засобах контролю, які підтримують ефективне управління інцидентами. Показники можуть кількісно оцінювати обсяг подій і співвідношення подій до інцидентів, інциденти за типом, продуктом, відділом, серйозністю тощо, своєчасність процесуального виконання для встановлення, розслідування та відхилення від задокументованих процедур.

Схвалені керівництвом політики та процедури для організацій і персоналу, які керують інцидентами, повинні включати чітко визначені ролі та обов’язки, включаючи інструкції щодо управління матеріалами для доказів із розслідування, зібраних із постраждалих систем, пристроїв, хмарних служб, програм і персоналу. Ці політики, процедури та допоміжні системи мають призвести до отримання юридично допустимих доказів.

Про інциденти безпеки надавачі послуг повинні повідомляти відповідні сторони, які постраждали, за допомогою заздалегідь визначених каналів зв’язку відповідно до відповідних правових, законодавчих та нормативних зобов’язань. При цьому слід чітко описати подію, яка сталася, її результат, а також визначити будь-які необхідні або рекомендовані дії для постраждалих сторін.

Висновки за розділом 3

В даному розділі було обґрунтовано необхідність оцінювання відповідності вимогам НХП та розглянуто наступні питання:

- вдосконалено стандартизований функційний підхід до процедури оцінки відповідності, ґрунтуючись на специфіці функціонування хмарних технологій;

- здійснено огляд існуючих фреймворків, які використовуються для оцінювання та сертифікації НХП щодо відповідності вимогам загальновизнаних стандартів безпеки;

- запропоновано розподіл на три рівні гарантій безпеки, яким повинен відповідати НХП при оцінюванні відповідності залежно від бізнес-потреб користувачів і критичності даних, які обробляє та зберігає хмарна інформаційна система;

- розроблено узагальнену схему вимог безпеки до НХП, побудовану на основі загальновідомих фреймворків, яка враховує різнорівневий підхід до гарантій безпеки, розподілену відповідальність за дотримання перерахованих вимог залежно від моделі функціонування і визначає компоненти архітектури хмари, які є чутливими до тих чи інших умов.

ВИСНОВОК

В ході даної дипломної роботи було вирішено актуальну проблему щодо розробки схеми вимог оцінювання інформаційної безпеки, релевантної до надавачів хмарних послуг, та процедури проведення оцінки їх відповідності для легітимізації використання хмарних технологій в організаціях різних форм власності та сфер діяльності.

Під час розв’язування завдань, які були поставлені для досягнення мети роботи, було отримано наступні результати:

1. Досліджено основні поняття технологій хмарних обчислень, їх різновиди та особливості функціонування. На підставі проведеного комплексу досліджень можна підсумувати, що при проектуванні безпеки хмарних систем важливо враховувати різні рівні логічної структури та зважати на моделі хмарних сервісів, адже вони відкривають різні точки входу в хмарні системи, які створюють неоднорідний ландшафт загроз інформаційній безпеці.

2. Проаналізовано загрози інформаційній безпеці, притаманні хмарним сервісам. Здійснений аналіз дає змогу зробити висновки, що вразливості традиційних інформаційних систем цілком можна екстраполювати на хмарну безпеку, а розглянуті загрози конгруентні з основними загальновідомими вимогами до захисту інформації. Відповідно, усі традиційні галузі безпеки залишаються, але характер ризиків, ролей і відповідальності, а також можливості управління і застосування засобів контролю значно змінюються.

3. Розглянуто основоположні стандарти та законодавчу базу України, які регулюють питання інформаційної безпеки хмарних сервісів. В рамках аналітичної роботи встановлено велике різноманіття іноземних стандартів, які регламентують вимоги до інформаційної безпеки. Провівши детальний аналіз нормативно-правової бази України, можна зробити висновок, що розробка державного законодавства для впровадження стратегії Cloud First орієнтується на міжнародні стандарти, що безумовно, полегшує впровадження хмари і підвищує безпеку за рахунок

використання найкращиї міжнародних практик безпеки, проте водночас існує загроза сліпого дублювання західних методологій, а такі шаблонні законопроекти, на жаль, не можуть повністю врахувати особливості українського законодавства і поточного стану ІТ-ринку держави.

4. Розроблено схему вимог для оцінювання інформаційної безпеки надавачів хмарних послуг. На базі розглянутих фреймворків та стандартів, було вдосконалено процедуру оцінки відповідності надавачів хмарних послуг, запропоновано трирівневий підхід до рівнів гарантій безпеки хмарних сервісів, а також здійснено розробку переліку вимог для оцінювання інформаційної безпеки надавачів хмарних послуг. Запропонований перелік, що ґрунтується на основних міжнародно визнаних стандартах, зменшує необхідність використання окремих схем сертифікації та значно спрощує планування, впровадження й оцінювання інформаційної безпеки надавачів хмарних послуг.

Таким чином, поставлені завдання було виконано в повному обсязі, що сприяло успішному досягненню поставленої мети роботи та забезпеченню практичної значущості отриманих результатів, що полягає в розробці структурованої сукупності рекомендацій, яким повинна відповідати інформаційна система надавачів хмарних послуг для ефективного забезпечення необхідного рівня інформаційної безпеки даних користувачів та визначення процедури їх оцінювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022 [Електронний ресурс] // Gartner, Inc., 19.04.2021. – Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022#:~:text=IaaS%2C%20DaaS%20and%20PaaS%20to,latest%20forecast%20from%20Gartner%2C%20Inc. – Назва з екрану.

2. NIST Special Publication 800-145, The NIST Definition of Cloud Computing [Електронний ресурс] – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

3. ISO/IEC 17788:2014 - Information technology — Cloud computing — Overview and vocabulary [Електронний ресурс] – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en.

4. Про хмарні послуги [Електронний ресурс] : Закон України від 17.02.2022 № 2075-IX. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2075-20#n69.

5. Жилін, А. Проблематика захисту інформаційних ресурсів при використанні хмарних технологій / А. Жилін, А. Дівіцький, А. Козачок // Information Technology and Security, 2019. – № 7 – p. 171–182.

6. The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 [Електронний ресурс] // CSA, 07.26.2017. – Режим доступу: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

7. NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture [Електронний ресурс] – Режим доступу: https://bigdatawg.nist.gov/_uploadfiles/M0008_v1_7256814129.pdf.

8. Sether, A. Cloud Computing Benefits [Електронний ресурс] / A. Sether // SSRN Electronic Journal, 2016. – № 11 – Режим доступу:

https://www.researchgate.net/publication/314530281_Cloud_Computing_Benefits#:~:text=Using%20different%20services%2C%20cloud%20computing,benefits%20of%20the%20cloud%20computing.

9. Rane, D. CSLAT: an SLA template for cloud service management [Електронний ресурс] / D. Rane, M. Sarma // International Journal of Communication Networks and Distributed Systems, 2015. – № 14(1) – Режим доступу: https://www.researchgate.net/publication/281667732_CSLAT_an_SLA_template_for_cloud_service_management.

10. Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025 [Електронний ресурс] // Gartner, Inc., 09.02.2021. – Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending. – Назва з екрану.

11. Subashini S. A survey on security issues in service delivery models of cloud computing / S. Subashini, V. Kavitha // Network Computer Application, 2010. – № 7 – p.11.

12. Naseer A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques / A. Naseer, H. Zhiqui, A. Ali// International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2017. – № 3 – p.55.

13. Eloff M. Internet of People, Things and Services – The Convergence of Security, Trust and Privacy / M. Dlamini, M. Eloff, J. Eloff // CompanionAble Workshop – IoPTS, 2009. – p.8.

14. ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс]. – Режим доступу: https://www.iso.org/isoiec-27001-information-security.html.

15. ISO/IEC 27017. Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002 [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/43757.html.

16. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/75652.html.

17. ISO/IEC 27018. Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/76559.html.

18. NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf.

19. NIST Cybersecurity Framework Version 1.1 [Електронний ресурс] – Режим доступу: https://www.nist.gov/cyberframework/framework.

20. Summary of the HIPAA Privacy Rule [Електронний ресурс] – Режим доступу: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

21. PCI Compliance Guide [Електронний ресурс] – Режим доступу: https://www.pcicomplianceguide.org/faq/.

22. Taylor, L. FedRAMP: History and future direction [Електронний ресурс] / L. Taylor // IEEE Cloud Computing, 2014. – № 1(10) – Режим доступу: https://www.researchgate.net/publication/273349891_FedRAMP_History_and_future_direction.

23. General Data Protection Regulation (GDPR) [Електронний ресурс] – Режим доступу: https://gdpr-info.eu/.

24. Пояснювальна записка до проекту Закону України "Про хмарні послуги" [Електронний ресурс] – Режим доступу: https://ips.ligazakon.net/document/view/GI01021A?an=2.

25. Волох, О. Обробка інформації в системах хмарних обчислень [Електронний ресурс] / О. Волох // Право і суспільство, 2016. – № 3 -– Режим доступу: http://pravoisuspilstvo.org.ua/archive/2016/3_2016/part_1/19.pdf.

26. Про державне регулювання діяльності щодо організації та проведення азартних ігор [Електронний ресурс] : Закон України від 14.07.2020 № 768-IX. – Режим доступу: https://zakon.rada.gov.ua/laws/show/768-20#Text.

27. Про інформацію [Електронний ресурс] : Закон України від 01.01.2022 № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

28. Про державну таємницю [Електронний ресурс] : Закон України від 15.03.2022 № 3855-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

29. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [Електронний ресурс]: Постанова КМУ від 08.07.2021 № 736-2016-п. – Режим доступу: https://zakon.rada.gov.ua/rada/show/736-2016-%D0%BF#Text.

30. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 01.01.2022 № 80/94-ВР. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#n99.

31. Про технічні регламенти та оцінку відповідності [Електронний ресурс] : Закон України від 19.02.2022 № 124-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/124-19#Text.

32. ДСТУ ISO/IEC 17000:2020 Оцінювання відповідності. Словник термінів і загальні принципи - Чинний від 2007-12-04. – Київ : Держспоживстандарт України, 2007. – 9 с.

33. 6 Reasons, why you Should Conduct Regular Security Assessments [Електронний ресурс] – Режим доступу: https://securetriad.io/importance-of-security-assessments/.

34. SOC 2 Compliance [Електронний ресурс] //Imperva, 12.07.2021. – Режим доступу: https://www.imperva.com/learn/data-security/soc-2-compliance/.

35. Матриця Cloud Controls і CAIQ v4 [Електронний ресурс] //CSA, 07.06.2021. – Режим доступу: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

36. EUCS – Cloud Services Scheme [Електронний ресурс] //ENISA, 22.12.2020. – Режим доступу: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

ДОДАТОК А

Таблиця 1

Організація інформаційної безпеки

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	+	+	+	+	+	+	+

1.1СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ		
№	**Опис вимог**	**Рівень гарантій**
1.1.1	НХП повинен визначати, впроваджувати, підтримувати та постійно вдосконалювати СУІБ, що охоплює принаймні оперативні підрозділи, місця, процеси для надання хмарних послуг та документувати всі заходи щодо цього.	БАЗОВИЙ
1.1.2	СУІБ має відповідати ДСТУ ISO/IEC 27001.	СЕРЕДНІЙ
1.1.3	СУІБ повинна мати дійсну сертифікацію відповідно до ДСТУ ISO/IEC 27001.	ВИСОКИЙ

продовження табл. 1

1.2КОНТАКТ З ВЛАДОЮ ТА ГРУПАМИ ІНТЕРЕСІВ		
1.2.1	НХП повинен бути в курсі поточних загроз і вразливостей.	БАЗОВИЙ
1.2.2	НХП періодично консультується з компетентними органами з точки зору інформаційної безпеки та відповідними технічними групами.	СЕРЕДНІЙ
1.2.3	Команда реагування НХП підтримує регулярний контакт CERT-UA, щоб бути в курсі поточних загроз і вразливостей.	ВИСОКИЙ
1.3НФОРМАЦІЙНА Б ЕЗПЕКА В УПРАВЛІННІ ПРОЕКТАМИ		
1.3.1	НХП повинен включати інформаційну безпеку в управління проектами, які можуть вплинути на безпеку, незалежно від характеру проекту.	БАЗОВИЙ
1.3.2	НХП виконує оцінку ризику відповідно до вимог управління ризиками для оцінки та керування ризиками в будь-якому проекті.	СЕРЕДНІЙ

Таблиця 2

Політика інформаційної безпеки

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	+	+	+	+	+	+	+

1.4ГЛОБАЛЬНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
№	**Опис вимог**	**Рівень гарантій**
1.4.1	НХП повинен затвердити та надати доступ до глобальної політики безпеки, яка охоплює принаймні наступні аспекти: - важливість інформаційної безпеки, виходячи з вимог бізнесу клієнтів; - цілі безпеки і бажаний рівень безпеки на основі бізнес-цілей користувачів; - зобов'язання НХП впроваджувати засоби безпеки для досягнення поставлених цілей безпеки; - найважливіші аспекти стратегії безпеки для досягнення поставлених цілей; - організаційна структура інформаційної безпеки в області застосування СУІБ.	БАЗОВИЙ
1.4.2	Перегляд глобальної ПІБ принаймні раз на рік.	СЕРЕДНІЙ
1.4.3	Перегляд глобальної ПІБ на регулярній основі або після істотних організаційних змін компанії, які можуть вплинути на принципи, визначені в ПІБ.	ВИСОКИЙ

продовження табл. 2

1.5ПОЛІТИКА ТА ПРОЦЕДУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
1.5.1	НХП повинен затвердити і надати доступ до політики та процедур, що випливають з глобальної ПІБ, для всіх задокументованих об'єктів, включаючи принаймні наступні аспекти: - цілі та сфера застосування; - ролі та відповідальність в організації, а також залежності з іншими організаціями; - кроки для виконання стратегії безпеки; - застосовні законодавчі та нормативні вимоги.	БАЗОВИЙ
1.5.2	Фахівці НХП повинні переглядати політику і процедури на відповідність принаймні щороку, після оновлення глобальної ПІБ або коли істотні зміни в середовищі можуть вплинути на безпеку хмарних сервісів. Зміни повинні бути затверджені до набуття чинності і повідомлені працівникам.	БАЗОВИЙ
1.5.3	Вище керівництво НХП затверджує політику та процедури або делегує це уповноваженим органам.	СЕРЕДНІЙ
1.5.4	У разі делегування уповноважені органи не рідше одного разу на рік звітують вищому керівництву про політику безпеки та її виконання.	ВИСОКИЙ

продовження табл. 2

1.6ВИНЯТКИ З ПІБ		
1.6.1	НХП повинен дотримуватись обмеженого в часі списку винятків з політик і процедур безпеки, включаючи пов’язані засоби контролю та переглядати його щонайменше один раз на рік.	БАЗОВИЙ
1.6.2	Затвердження переліку відбувається щонайменше один раз на рік, навіть якщо перелік не оновлювався.	СЕРЕДНІЙ
1.6.3	Винятки підлягають процесу управління ризиками, включаючи схвалення цих винятків та прийняття відповідних ризиків і їх власників.	СЕРЕДНІЙ
1.6.4	Винятки з політик і процедур безпеки затверджуються вищим керівництвом або уповноваженим органом.	ВИСОКИЙ
1.6.5	Список винятків оновлюється автоматично, щоб гарантувати, що термін дії затверджених винятків не закінчився, а всі перевірки та затвердження залишаються актуальними.	ВИСОКИЙ

Таблиця 3

Аудит та відповідність вимогам

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	+	-	-	-	+	+	-

1.7ІДЕНТИФІКАЦІЯ ВИМОГ ВІДПОВІДНОСТІ		
№	**Опис вимог**	**Рівень гарантій**
1.7.1	НХП повинен задокументувати юридичні, нормативні, самостійно визначені та договірні вимоги, що стосуються інформаційної безпеки.	БАЗОВИЙ
1.7.2	НХП повинен задокументувати та впровадити процедури для відповідності цим умовам.	СЕРЕДНІЙ
1.7.3	НХП здійснює активний моніторинг правових, нормативних та договірних вимог до хмарних послуг	ВИСОКИЙ

продовження табл. 3

1.8ПОЛІТИКА ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ АУДИТІВ		
1.8.1	НХП повинен документувати, повідомляти та впроваджувати політику та процедури для планування й проведення аудитів, зроблені відповідно до політик і процедур безпеки, що стосуються наступних аспектів: - обмеження доступу лише для читання до компонентів системи відповідно до узгодженого плану аудиту та за необхідності для виконання заходів безпеки; - дії, які можуть привести до збоїв у роботі хмарного сервісу або порушення договірних вимог, виконуються під час планового технічного обслуговування або поза піковими періодами; - обов’язкова реєстрація та моніторинг діяльності під час проведення аудиту	БАЗОВИЙ
1.8.2	НХП повинен задокументувати та впровадити програму аудиту протягом трьох років, яка визначає обсяг і частоту аудиту відповідно до управління змінами, ПІБ та результатів оцінки ризику.	СЕРЕДНІЙ
1.8.3	НХП надає користувачам хмарних послуг гарантовану контрактом інформацію та визначає їхні права на аудит.	ВИСОКИЙ

продовження табл. 3

1.9СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ		
1.9.1	НХП повинен проводити через регулярні проміжки часу принаймні раз на рік внутрішні аудити експертами інформаційної безпеки для перевірки відповідності їх системи внутрішнього контролю безпеки вимогам, що визначені пунктом «Ідентифікація вимог відповідності».	БАЗОВИЙ
1.9.2	Виявлені вразливі місця та відхилення підлягають оцінці ризику відповідно до процедури управління ризиками, а подальші заходи з їх оцінки і усунення визначаються та відстежуються.	СЕРЕДНІЙ
1.9.3	Внутрішній аудит повинен бути доповнений процедурами для автоматичного контролю за дотриманням застосовних вимог політики та інструкцій.	ВИСОКИЙ
1.9.4	НХП повинен впровадити автоматизований моніторинг для виявлення вразливостей і відхилень, про що автоматично повідомляються відповідні експерти НХП для негайної оцінки та вжиття заходів.	ВИСОКИЙ
1.9.5	НХП зобов’язаний інформувати користувача хмарних послуг про невідповідності вимогам.	СЕРЕДНІЙ
1.9.6	НХП регулярно інформує своє вище керівництво про показники інформаційної безпеки в рамках системи внутрішнього контролю.	БАЗОВИЙ

ДОДАТОК Б

Таблиця 4

Управління активами

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	+	-	-	-	-	-	-

2.1ІНВЕНТАРИЗАЦІЯ АКТИВІВ		
№	**Опис вимог**	**Рівень гарантій**
2.1.1	НХП повинен документувати та впроваджувати політику та процедури для ведення інвентаризації активів організації і реєструвати для кожного активу інформацію, необхідну для застосування процедури управління ризиками – визначення активу, функції, модель, версія, місцезнаходження.	БАЗОВИЙ
2.1.2	Інвентаризація повинна виконуватися автоматично та/або людьми або командами, відповідальними за активи, щоб забезпечити повну, точну та послідовну інвентаризацію, реєстрацію змін та впровадження заходів з управління ризиками протягом у сього життєвого циклу активу.	СЕРЕДНІЙ
2.1.3	НХП автоматично контролює інвентаризацію активів, щоб гарантувати її актуальність, а інформація про активи повинна розглядатися програмами моніторингу для виявлення шкідливого впливу на хмарні послуги	ВИСОКИЙ

продовження табл. 4

2.2ПОЛІТИКА БЕЗПЕЧНОГО КОРИСТУВАННЯ АКТИВАМИ		
2.2.1	НХП повинен документувати та впроваджувати політику та процедури для прийнятного використання і безпечного поводження з активами.	БАЗОВИЙ
2.2.2	Політика та процедури користування активами повинна враховувати весь життєвий цикл активів.	СЕРЕДНІЙ
2.2.3	Якщо портативний носій використовується в технічній інфраструктурі або для завдань адміністрування, цей носій має бути призначений для одноразового використання.	ВИСОКИЙ
2.3ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ ОБЛАДНАННЯ		
2.3.1	НХП повинен документувати та впровадити політику та процедури введення в експлуатацію обладнання, шо використовується для надання хмарних послуг у виробничому середовищі, яка повинна включати початкову перевірку безпечної конфігурації механізмів обробки помилок, реєстрацію, шифрування, автентифікацію та авторизацію активів відповідно до цілей користування.	БАЗОВИЙ
2.3.2	Процедура введення в експлуатацію повинна гарантувати, що ризики, пов’язані введенням активу будуть ідентифіковані, проаналізовані та пом’якшені.	СЕРЕДНІЙ
2.3.3	Схвалення введення в експлуатацію та виведення з експлуатації обладнання має бути задокументовано в цифровому вигляді та контролюватися автоматично.	ВИСОКИЙ

продовження табл. 4

2.3.4	НХП повинен визначити схему класифікації активів, яка відображає потреби в захисті інформації, що обробляє, зберігає або передає кожен актив та маркувати всі можливі активи відповідно до їх класифікації.	БАЗОВИЙ
2.3.5	Схема класифікації активів повинна забезпечувати відповідні рівні захисту для цілей забезпечення конфіденційності, цілісності, доступності та автентичності даних.	СЕРЕДНІЙ
2.4ВИКОРИСТАННЯ ТА ПОВЕРНЕННЯ АКТИВІВ		
2.4.1	НХП забезпечує та документує, що всі внутрішні та зовнішні працівники відповідають політикам прийнятного використання та безпечного поводження з активами.	БАЗОВИЙ
2.4.2	Процедури користування активами повинні передбачати заходи для забезпечення виведення з експлуатації апаратного забезпечення (надійне видалення даних або належне знищення носія) та повернення всіх активів, якими користуються працівники.	БАЗОВИЙ
2.4.3	НХП централізовано та автоматизовано керує активами, якими користуються зовнішні та внутрішні співробітники, включаючи АЗ, ПЗ і дані, на які розповсюджується політика, забезпечує їх віддалену дезактивацію, видалення або блокування.	ВИСОКИЙ

Таблиця 5

Управління персоналом

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	-	-	-	-	-	-	+

2.5УПРАВЛІННЯ ПЕРСОНАЛОМ		
№	**Опис вимог**	**Рівень гарантій**
2.5.1	НХП повинен класифікувати чутливі до інформаційної безпеки посади відповідно до рівня їх ризику, включаючи посади, пов'язані з адмініструванням IT та наданням хмарних послуг у виробничому середовищі, а також усі посади з доступом до даних клієнта хмари або компонентів системи.	БАЗОВИЙ
2.5.2	НХП має включати у свої трудові договори або спеціальні кодекси поведінки загальну угоду внутрішніх і зовнішніх співробітників щодо етичного виконання своїх професійних обов'язків та перевіряти рівень їх компетентності перед початком роботи, вимоги яких повинні переглядатись щорічно і адаптуватись за необхідністю. Обсяг перевірки має бути пропорційним бізнес-контексту, конфіденційності інформації, до якої працівник отримає доступ, і пов'язаних ризиків	БАЗОВИЙ

продовження табл. 5

2.5.3	НХП має задокументувати процедури, які необхідно вжити у разі порушення ПІБ та інструкцій кодексу етики або застосовних нормативних вимог, включаючи перевірку, чи сталося порушення, розгляд його характеру рівень впливу і передбачувані дисциплінарні заходи.	БАЗОВИЙ
2.5.4	Компетентність та доброчесність внутрішніх і зовнішніх співробітників НХП повинна бути перевірена перед початком роботи при переході на посаду з вищою класифікацією ризику.	СЕРЕДНІЙ
2.5.5	Компетентність та доброчесність внутрішніх і зовнішніх співробітників НХП щорічно перевіряється для працівників, які займають посади з найвищим рівнем класифікації ризику.	ВИСОКИЙ
2.6УМОВИ ПРАЦІВНИКА		
2.6.1	НХП гарантує, що внутрішні та зовнішні співробітники зобов’язані дотримуватись всіх застосовних політик і процедур інформаційної безпеки.	БАЗОВИЙ
2.6.2	НХП гарантує, що у мови працевлаштування для всіх внутрішніх і зовнішніх співробітників включають положення про нерозголошення, яке охоплює будь-яку інформацію, що була отримана або створена як частина хмарної служби, навіть якщо вона анонімізована та деконтекстуалізована.	БАЗОВИЙ
2.6.3	Усі внутрішні та зовнішні співробітники повинні визнати в задокументованій формі представлені їм політики та процедури інформаційної безпеки, перш ніж їм буде надано будь-який доступ до даних клієнтів, виробничого середовища або будь-якого їх компонента.	СЕРЕДНІЙ

продовження табл. 5

2.6.4	Перевірка підтвердження повинна контролюватися автоматично в процесах і автоматизованих системах, що використовуються для надання прав доступу співробітникам.	ВИСОКИЙ
2.6.5	НХП повідомляє працівників і застосовує особливу процедуру для відкликання прав доступу і активів співробітників, коли їх робота припиняється або змінюється.	БАЗОВИЙ
2.6.6	Процедури після припинення роботи визначає конкретні ролі та обов'язки і включає задокументований список необхідних кроків.	СЕРЕДНІЙ
2.6.7	НХП автоматично контролює застосування процедури припинення роботи.	ВИСОКИЙ
2.7НАВЧАННЯ ТА ОБІЗНАНІСТЬ ПРАЦІВНИКІВ		
2.8.1	НХП визначає програму підвищення обізнаності та навчання щодо безпеки, яка охоплює системні компоненти, обробку даних користувачів та поведінку в разі виникнення інцидентів безпеки.	БАЗОВИЙ
2.8.2	Програма навчання працівників визначена з врахуванням ризиків посади та технічних обов'язків.	СЕРЕДНІЙ
2.8.3	НХП контролює виконання програми навчання і вимірює її результати.	СЕРЕДНІЙ
2.8.4	НХП перевіряє ефективність програми навчання з безпеки, використовуючи практичні вправи та імітацію кібератак.	ВИСОКИЙ

ДОДАТОК В

Таблиця 6

Управління ризиками

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	+	+	+	+	+	+	+

3.1ПОЛІТИКА УПРАВЛІННЯ РИЗИКАМИ		
№	**Опис вимог**	**Рівень гарантій**
3.1.1	НХП повинен задокументувати політику управління ризиками для таких аспектів: - ідентифікація ризиків, пов'язаних із втратою конфіденційності, цілісності, доступності та достовірності інформації в рамках СУІБ та присвоєння власних ризиків; - аналіз ймовірності, впливу та визначення рівня ризиків; - аналіз ризиків на основі критеріїв прийняття ризику та визначення пріоритетів їх обробки; - прийняття залишкових ризиків та документування впроваджених заходів.	БАЗОВИЙ
3.1.2	НХП має використовувати документований метод аналізу ризиків, який гарантує відтворюваність і порівнянність підходу мінімізації ризиків.	СЕРЕДНІЙ

продовження табл. 6

3.2ВПРОВАДЖЕННЯ ОЦІНКИ ТА ОБЛІКУ РИЗИКІВ		
3.2.1	НХП повинен впроваджувати політику та процедури, що охоплюють оцінку ризиків по всьому периметру хмарного сервісу та надавати результати оцінки зацікавленим сторонам.	БАЗОВИЙ
3.2.2	Обсяг визначення ризику повинен включати наступні аспекти: різні потреби захисту даних користувачів, появу слабких місць, збоїв і несправностей у технічних захисних засобах, конфліктні завдання та сфери відповідальності, а також залежність від субсервісних організацій.	БАЗОВИЙ
3.2.3	НХП переглядає оцінку ризиків щонайменше раз на рік та після кожної значної зміни, яка може впливати на безпеку хмарного сервісу.	СЕРЕДНІЙ
3.2.4	НХП повинен відстежувати розвиток факторів ризику та переглядати результати оцінки ризику.	ВИСОКИЙ
3.2.5	НХП має визначати та реалізувати план щодо оброблення ризиків відповідно до рівня їх пріоритету за рівнем критичності шляхом їх зменшення або уникнення за допомогою контролю безпеки, розподілу або збереження. НХП визначає пріоритети ризиків.	БАЗОВИЙ
3.2.6	НХП надає план обробки ризиків доступним для відповідних зацікавлених сторін. План обробки ризиків повинен знизити рівень ризику до порогового значення, яке вважається прийнятним для власників ризику.	БАЗОВИЙ
3.2.7	Власники ризиків повинні офіційно затвердити план мінімізації ризиків, зокрема, прийняття залишкового ризику.	СЕРЕДНІЙ

продовження табл. 6

3.2.8	Якщо НХП поділяє ризики з клієнтами, спільні ризики повинні бути вказані в документації користувача.	СЕРЕДНІЙ
3.2.9	НХП переглядає план обробки ризиків щоразу, коли переглядається оцінка ризику.	БАЗОВИЙ
3.2.10	Власники ризиків перевіряють на адекватність аналіз, оцінку та обробку ризиків, включаючи схвалення та прийняття залишкових ризиків після кожного перегляду планів оцінки ризиків та їх усунення.	СЕРЕДНІЙ

Таблиця 7

Управління змінами та конфігураціями

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	+	+	+	+	+	-	-
3.ЗПОЛІТИКА УПРАВЛІННЯ ЗМІНАМИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ									
№	**Опис вимог**								**Рівень гарантій**
3.3.1	НХП повинен документувати, впроваджувати та повідомляти про політики та процедури для управління змінами в інформаційних системах, що підтримують хмарні сервіси.								БАЗОВИЙ

продовження табл. 7

3.3.2	Політика та процедури управління змінами повинні охоплювати аспекти критеріїв та оцінки ризику, категоризації та визначення пріоритетності змін і відповідні вимоги до типу та обсягу попередніх випробувань, вимоги щодо документації змін у системі та розподілу обов'язків під час планування, тестування і впровадження змін.	СЕРЕДНІЙ
3.3.3	НХП має класифікувати зміни та розставити пріоритети з огляду на потенційний вплив безпеки на компоненти системи. Класифікація та визначення пріоритетів відбувається на основі оцінки ризику.	БАЗОВИЙ
3.3.4	Якщо ризик пов'язаний із запланованими змінами високий, необхідно вжити заходів для його пом'якшення.	СЕРЕДНІЙ
3.3.5	НХП інформує користувачів хмарних послуг щодо змін, які мають високу категорію ризику.	ВИСОКИЙ
3.4ТЕСТУВАННЯ ЗМІН		
3.4.1	НХП повинен документувати і тестувати заплановані зміни перед розгортанням. Тип і обсяг випробувань повинні відповідати оцінці ризику.	БАЗОВИЙ
3.4.2	НХП повинен отримати згоду клієнтів, анонімізувати дані, перед використанням їх при тестуванні.	СЕРЕДНІЙ
3.4.3	Перед розгортанням змін на системному компоненті НХП повинен виконати регресійне тестування інших компонентів хмарного сервісу, які залежать від цього компонента системи, щоб перевірити відсутність небажаних ефектів.	ВИСОКИЙ
3.4.4	НХП повинен автоматично контролювати визначення та виконання тестів щодо змін і виправлення проблем в системі та виробничому середовищі.	ВИСОКИЙ

продовження табл. 7

3.5ВПРОВАДЖЕННЯ ЗМІН		
3.5.1	НХП визначає роль та права для уповноваженого персоналу та компонентів системи, яким дозволено вносити зміни до хмарної служби у виробничому середовищі. Усі зміни в хмарному сервісі мають реєструватися та відстежуватися до системного компонента, який ініціював цю зміну.	БАЗОВИЙ
3.5.2	НХП повинен автоматично контролювати зміни у виробничому середовищі, щоб гарантувати виконання політики управління змінами.	ВИСОКИЙ
3.5.3	НЗП має реалізувати процедури контрою версій для відстеження окремих змін і відновлення уражених компонентів системи до їх попереднього стану і результаті виникнення помилок або виявлених вразливостей.	БАЗОВИЙ
3.5.4	Процедури контролю версій повинні передбачати відповідні запобіжні заходи, щоб гарантувати безпеку даних клієнтів при поверненні до попереднього стану системи.	ВИСОКИЙ

Таблиця 8

Управління ланцюгами поставок

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	+	+	+	+	+	-	-

3.6ПОЛІТИКА КОНТРОЛЮ ТРЕТІХ СТОРІН		
№	**Опис вимог**	**Рівень гарантій**
3.6.1	НХП повинен впроваджувати політику та процедури для контролю та моніторингу третіх сторін, чиї продукти чи послуги сприяють наданні хмарного сервісу.	БАЗОВИЙ
3.6.2	НХП за контрактом може вимагати від своїх субсервісних організацій надавати регулярний звіт незалежних аудиторів про відповідність та ефективність роботи їхньої системи внутрішнього контролю безпеки, пов'язаної з хмарними послугами, що надаються.	СЕРЕДНІЙ
3.6.3	Якщо організації-постачальники не можуть надати звіт про відповідність вимогам, НХП залишає за собою право проводити аудит для оцінки придатності та ефективності їхньої системи безпеки.	ВИСОКИЙ
3.7ВЗАЄМОДІЯ З ПОСТАЧАЛЬНИКАМИ		
3.7.1	НХП підтримує каталог для моніторингу постачальників, які сприяють наданню хмарних послуг і регулярно виконує оцінку ризиків та моніторинг вимог інформаційної безпеки своїх постачальників відповідно до процедур моніторингу третіх сторін, перш ніж використовувати їхні послуги.	БАЗОВИЙ

продовження табл. 8

3.7.2	НХП повинен гарантувати, що постачальник субпослуг надав докази, що підтверджують оцінку їх ефективності до цільового рівня оцінки.	СЕРЕДНІЙ
3.7.3	НХП доповнює процедури контролю за дотриманням автоматичного моніторингу конфігурацій компонентів системи, продуктивності компонентів, час реагування на інциденти безпеки і час відновлення та автоматично відстежує виявлення порушень..	ВИСОКИЙ
3.7.4	НХП повинен визначити стратегію відмови від закупівлі послуг третьої сторони	БАЗОВИЙ

Таблиця 2

Безперервність бізнесу

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	+	+	+	+	+	+	-

3.8ПОЛІТИКА БЕЗПЕРЕРВНОСТІ БІЗНЕСУ		
№	**Опис вимог**	**Рівень гарантій**
3.8.1	НХП повинен задокументувати і зробити доступними політики і процедури, що встановлюють стратегію та керівні принципи для забезпечення безперервності бізнесу та управління непередбачуваними ситуаціями, які включають необхідність аналізу впливу будь-якої несправності на бізнес НХП та користувача хмарних послуг.	БАЗОВИЙ
3.8.2	НХП має призначити власника процесу безперервності бізнесу і управління непередбачуваними ситуаціями, який буде відповідальним за виконання інструкцій і забезпечення наявності достатніх ресурсів з реалізації стратегії безперервності бізнесу.	СЕРЕДНІЙ
3.8.3	Аналіз впливу на бізнес повинен переглядатись регулярно принаймні один раз на рік або після значних організаційних змін.	СЕРЕДНІЙ

продовження табл. 9

3.9ПЛАН БЕЗПЕРЕРВНОСТІ БІЗНЕСУ		
3.9.1	НХП повинен задокументувати та впровадити план безперервності бізнесу та плани на випадок надзвичайних ситуацій для забезпечення безперервності послуг, враховуючи обмеження інформаційної безпеки та результати аналізу впливу на бізнес.	БАЗОВИЙ
3.9.2	План безперервності бізнесу повинен переглядатися регулярно принаймні раз на рік або після значних організаційних змін та визначати мету та обсяг, включаючи відповідні бізнес-процеси і залежності, зрозумілий план дій для осіб, відповідальних за його виконання, канали повідомлення клієнтів, процедури відновлення та інтерфейси управління інцидентами безпеки.	СЕРЕДНІЙ
3.9.3	Аналіз впливу на бізнес і план безперервності бізнесу повинні регулярно проходити тестування, результати якого повинні бути задокументовані та враховані для вдосконалення системи.	БАЗОВИЙ
3.9.4	Для тестування можуть залучатись відповідні треті сторони і користувачі хмарних послуг.	СЕРЕДНІЙ
3.9.5	На додаток до випробувань проводяться вправи, які базуються на сценаріях інцидентів безпеки, яких зазнавав НХП.	ВИСОКИЙ

Таблиця 3

Сумісність і портативність

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	НХП	-	-	-	-	+	+	-

3.10 ДОКУМЕНТАЦІЯ ТА БЕЗПЕКА ІНТЕРФЕЙСІВ ВВОДУ-ВИВОДУ		
№	**Опис вимог**	**Рівень гарантій**
3.10.1	Хмарний сервіс повинен бути доступним для хмарних служб інших НХП або інформаційних систем хмарних клієнтів через задокументовані вхідні та вихідні інтерфейси. Зв'язок на цих інтерфейсах має використовувати стандартизовані протоколи, які забезпечують конфіденційність і цілісність переданої інформації відповідно до вимог її захисту.	БАЗОВИЙ
3.10.2	Зв'язок через ненадійні мережі має бути зашифрований згідно вимог криптографічного захисту.	СЕРЕДНІЙ
3.10.3	НХП дозволяє своїм клієнтам перевіряти надані інтерфейси та їх безпеку на відповідність вимогам захисту перед початком використання хмарних сервісів.	ВИСОКИЙ

продовження табл. 10

3.11 ДОГОВІРНІ УГОДИ ПРО НАДАННЯ ДАНИХ		
3.11.1	НХП повинен включати в договірні угоди про хмарні послуги аспекти про тип, обсяг, формат даних, що надаються клієнту, способи їх доставки, визначення термінів надання, процедур видалення, а також обов’язки та зобов’язання користувача щодо співпраці для надання даних.	БАЗОВИЙ
3.11.2	Визначення умов договірних угод повинні ґрунтуватися на потребах експертів потенційних клієнтів, які оцінюють придатність хмарного сервісу щодо відповідності до нормативних вимог.	СЕРЕДНІЙ
3.11.3	НХП повинен регулярно визначати правові та нормативні вимоги до надання даних і відповідно коригувати договірні угоди.	ВИСОКИЙ

ДОДАТОК Г

Таблиця 11

Безпека фізичної інфраструктури та віртуальних мереж

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
НХП	НХП	НХП	+	+	-	-	-	-	-

4.1ПЕРИМЕТРИ БЕЗПЕКИ		
№	**Опис вимог**	**Рівень гарантій**
4.1.1	НХП повинен визначити периметри безпеки в будівлях і приміщеннях, що стосуються надання хмарних послуг та щонайменш дві зони безпеки, одна з яких охоплює всі будівлі та приміщення, а інша – чутливі види діяльності, такі як приміщення інформаційної системи для виробництва хмарних послуг або місця, де здійснюється обробка та зберігання клієнтських даних, а також розробка та адміністрування інформаційних систем.	БАЗОВИЙ
4.1.2	НХП забезпечує відсутність прямого доступу між зоною загального користування та чутливими зонами, доступ до яких вимагає використання багатофакторної автентифікації.	ВИСОКИЙ

продовження табл. 11

4.1.3	НХП повинен захищати та відстежувати доступ до периметрів зон безпеки технічними засобами безпеки та включати реєстрацію всіх доступів, як користувачів і відвідувачів, так і персоналу, до непублічних зон для своєчасного виявлення та запобігання несанкціонованому доступу.	БАЗОВИЙ
4.1.4	НХП визначає співвідношення між активами, діяльністю та зонами, що вказує які активи або дії можуть/не мають/повинні використовуватись в кожній зоні безпеки. Політика контролю доступу повинна описувати часові проміжки та умови доступу до кожної зони відповідно до профілів користувачів та рівня критичності зони. Реєстрація доступу контролюється автоматично.	ВИСОКИЙ
4.1.5	НХП повинен забезпечити захист хоста та гостьову операційну систему, гіпервізор та рівень управління інфраструктурою відповідно до відповідних найкращих практик і за підтримки технічного контролю, як частину базової лінії безпеки.	БАЗОВИЙ
4.2ЗАХИСТ ОБЛАДНАННЯ		
4.2.1	НХП повинен документувати та впроваджувати політику та процедури щодо захисту обладнання, включаючи захист кабелів живлення та зв’язку від перехоплення, перешкод або пошкодження, захист обладнання під час технічного обслуговування, захист обладнання, що зберігає дані клієнтів під час транспортування.	БАЗОВИЙ
4.2.2	Процедури захисту обладнання повинні включати перевірку захисту, яку слід виконувати щонайменше кожні два роки, а також у разі підозри на шкідливі маніпуляції.	СЕРЕДНІЙ

продовження табл. 11

4.2.3	Політики та процедури захисту обладнання повинні включати заходи забезпечення того, щоб умови встановлення, технічного обслуговування обладнання були сумісними з вимогами доступності та безпеки хмарного сервісу.	ВИСОКИЙ
4.2.4	НХП повинен гарантувати, що угоди про технічне обслуговування обладнання, яке використовується для хмарної служби, дають змогу вчасно встановлювати оновлення безпеки на цьому обладнанні.	ВИСОКИЙ
4.2.5	НХП повинен задокументувати набір вимог безпеки, пов’язаних із зовнішніми й екологічними загрозами та надавати хмарну послугу принаймні з двох місць, які відокремлені на достатню відстань і забезпечують один одному оперативну резервність та стійкість.	БАЗОВИЙ
4.2.6	Вимоги безпеки для ЦОД повинні ґрунтуватися на критеріях, які відповідають встановленим правилам технології та включати часові обмеження для самодостатньої роботи у разі надзвичайних ситуацій і максимально допустимий час простою. НХП повинен регулярно перевіряти ефективність резервування.	СЕРЕДНІЙ
4.2.7	Вимоги безпеки до ЦОД повинні включати випробування обладнання фізичного захисту принаймні один раз на рік.	ВИСОКИЙ

продовження табл. 11

4.ЗБЕЗПЕКА КІНЦЕВИХ ТОЧОК									
Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	НХП	+	-	-	-	-	-	-

№	Опис вимог	Рівень гарантій
4.3.1	НХП повинен регулярно проводити інвентаризацію кінцевих точок і застосовувати політики і процедури безпеки для всіх кінцевих точок, до яких дозволено доступ системи та тих, що зберігають, передають або обробляють організаційні дані. Всі кінцеві точки повинні бути захищені за допомогою правильно налаштованих брандмауерів, DLP-систем та технологій виявлення і запобігання ШПЗ.	БАЗОВИЙ
4.3.2	НХП повинен визначити, задокументувати, застосувати та оцінити перелік схвалених послуг, програм та джерел програм, прийнятних для використання кінцевими точками при доступі або зберіганні даних, керованих організацією, а також процес перевірки кінцевої точки на сумісність пристрою з ОС та програмами.	СЕРЕДНІЙ
4.3.3	НХП повинен впроваджувати процедури та технічні заходи, що дозволяють вмикати геолокацію та віддалено видаляти дані на керованій кінцевій точці пристроїв, а також передбачити договірні засади для підтримки безпеки кінцевих точок третіх сторін з доступом до активів організації.	ВИСОКИЙ

продовження табл. 11

4.4БЕЗПЕКА ДОДАТКІВ									
Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	НХП	-	-	-	-	+	-	-

№	**Опис вимог**	**Рівень гарантій**
4.4.1	НХП повинен встановити та підтримувати політики і процедури безпеки додатків відповідно до визначених бізнес-цілей.	БАЗОВИЙ
4.4.2	Політика безпеки додатків має враховувати безпеку в розробці, розгортання ПЗ (включаючи безперервну доставку), безпеку в експлуатації (впровадження оновлень при виявлених вразливостях), а також стандарти безпечного кодування, для уникнення вразливостей, прихованих у коді програми.	СЕРЕДНІЙ
4.4.3	НХП повинен автоматизовано підтримувати список залежностей від апаратних та програмних продуктів, які використовуються при розробці його хмарного сервісу і надавати його клієнтам за запитом.	ВИСОКИЙ
4.4.4	НХП повинен документувати та впроваджувати політику щодо використання стороннього ПЗ та ПЗ з відкритим кодом, враховуючи аспекти обмежень щодо прийнятних ліцензій, застарілих компонентів та версій з відомими вразливостями.	ВИСОКИЙ

продовження табл. 11

4.4.5	Політика і процедури безпеки додатків повинні гарантувати інформаційну безпеку хмарних сервісів при проектуванні та на всіх етапах розробки, забезпечити конфіденційність і цілісність вихідного коду. НХП повинен використовувати контроль версій для збереження історій змін ПЗ.	СЕРЕДНІЙ
4.4.6	НХП повинен впроваджувати процедури для розробки функцій безпеки додатків, які реалізують технічні механізми або запобіжні заходи безпеки, включаючи специфікацію очікуваних вхідних/вихідних даних, можливих помилок і аналіз ефективності запланованих функцій.	ВИСОКИЙ
4.4.7	Процедури виявлення вразливостей повинні бути інгтегровані в процес розробки, а саме статичне/динамічне тестування безпеки програми та огляд коду експертами.	СЕРЕДНІЙ
4.4.8	Перевірки коду й тести на проникнення повинні регулярно проводитися кваліфікованим персоналом або підрядниками, , а виявлені вразливості – оцінюватись та усуватись.	ВИСОКИЙ

продовження табл. 11

4.5БЕЗПЕКА ДАНИХ									
Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	-	-	-	-	-	+	-

№	**Опис вимог**	**Рівень гарантій**
4.5.1	НХП повинен встановити та підтримувати політику та процедури класифікації, захисту та обробки даних протягом усього життєвого циклу відповідно до всіх застосовних законів та стандартів. Зберігання, архівування та видалення даних повинні здійснюватися за визначеними процедурами.	БАЗОВИЙ
4.5.3	Дані повинні бути інвентаризовані, разом із документуванням їх фізичного розташування, обробки і збереження резервних копій, та класифіковані відповідно до їх типу та рівня чутливості.	СЕРЕДНІЙ
4.5.4	НХП повинен описати процедури розкриття даних на запит правоохоронних органів.	ВИСОКИЙ
4.5.5	НХП впроваджує процедури видалення даних клієнтів при розірванні їх договору відповідно до договірних угод між ними.	БАЗОВИЙ
4.5.6	Процедури видалення даних клієнта хмари повинні перешкоджати відновленню за допомогою спеціальних засобів.	СЕРЕДНІЙ
4.5.7	НХП повинен документувати видалення даних, метаданих і резервних копій таким чином, щоб клієнт хмарних послуг відстежував ці процедури.	ВИСОКИЙ

продовження табл. 11

4.6БЕЗПЕКА МЕРЕЖІ									
Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	+	+	-	-	-	+	-

№	**Опис вимог**	**Рівень гарантій**
4.6.1	НХП повинен впроваджувати технічні засоби захисту, які ґрунтуються на результатах аналізу ризику, для швидкого виявлення та реагування на мережеві атаки для забезпечення захисту інформації та систем обробки інформації.	БАЗОВИЙ
4.6.2	НХП має подавати в систему SIEM усі дані з технічних заходів безпеки, які впроваджуються, щоб ініціювати автоматичні контрзаходи щодо корелюючих подій.	СЕРЕДНІЙ
4.6.3	НХП повинен документувати та впроваджувати конкретні вимоги безпеки для підключення в межах мережі та процедури з технічними та організаційними гарантіями захисту передачі даних.	БАЗОВИЙ
4.6.4	НХП впроваджує окремі мережі для адміністративного управління, розділяє надійні та ненадійні мережі на різні зони безпеки для внутрішніх і зовнішніх мереж та розроблює як фізичне, так і віртуалізоване мережеве середовище для обмеження з'єднань. Кожен периметр мережі контролюється шлюзами безпеки.	БАЗОВИЙ

продовження табл. 11

4.6.5	НХП регулярно переглядає проект, впровадження та конфігурацію мереж для моніторингу з’єднань з урахуванням визначених вимог безпеки.	СЕРЕДНІЙ
4.6.6	НХП повинен визначати, документувати та впроваджувати механізми поділу на мережевому рівні трафіку даних різних клієнтів хмари.	БАЗОВИЙ
4.6.7	Безпечна сегрегація повинна бути забезпечена фізично відокремленими мережами або надійно зашифрованими VLAN.	ВИСОКИЙ
4.6.8	Шлюзи безпеки дозволяють лише легітимні з’єднання, визначені в матриці авторизованих потоків, а авторизація доступу до системи для міжмережного доступу базується на оцінці безпеки на основі вимог хмарних клієнтів.	СЕРЕДНІЙ
4.6.9	Кожен периметр мережі повинен автоматично контролюватися резервними високодоступними шлюзами безпеки.	ВИСОКИЙ
4.6.10	НХП повинен підтримувати в актуальному стані документацію щодо логічної структури мережі, яка охоплює інформацію про сегментацію, географічне розташування та інвентаризацію активів.	БАЗОВИЙ

ДОДАТОК Ґ

Таблиця 12

Управління ідентифікацією, автентифікацією та контролем доступу

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	-	+	-	-	+	+	+

5.1ПОЛІТИКА КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЇ		
№	**Опис вимог**	**Рівень гарантій**
5.1.1	НХП повинен впроваджувати політику та процедури щодо ролей та прав для контролю доступу до інформаційних ресурсів на основі вимог бізнесу та безпеки, враховуючи принцип «найменших привілеїв», використовуючи рольовий механізм для призначення прав доступу, спеціальні правила для користувачів з привілейованим доступом, а також розподіл обов'язків між керуванням, схваленням та призначенням прав доступу.	БАЗОВИЙ
5.1.2	НХП повинен спроектувати, розробити, налаштувати і розгорнути хмарну інформаційну систему, щоб відокремити технічну інфраструктуру та обладнання, необхідне для адміністрування хмарної служби й активів, які вона розміщує.	СЕРЕДНІЙ

продовження табл. 12

5.2УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ КОРИСТУВАЧІВ		
5.2.1	НХП повинен задокументувати політику управління ОЗ користувачів, в якій описано аспекти призначення унікальних імен, визначення різних підтримуваних типів ОЗ, призначення параметрів ролей контролю доступу для кожного типу, а також події, що призводять до блокування ОЗ.	БАЗОВИЙ
5.2.2	НХП повинен задокументувати політику для керування ОЗ, в якій описані розподіл обов'язків між керуванням, схваленням та призначенням ОЗ користувачів, регулярна перевірка призначених ОЗ і пов'язаних прав доступу, блокування і відкликання ОЗ у разі бездіяльності або компрометації.	СЕРЕДНІЙ
5.2.3	НХП повинен запропонувати користувачам самообслуговування, за допомогою якого вони можуть самостійно керувати ОЗ всіх користувачів під їх відповідальність.	СЕРЕДНІЙ
5.2.4	НХП повинен визначити і впровадити автоматизований механізм блокування та відкликання ОЗ користувачів через певний період часу або після певної кількості невдалих спроб автентифікації.	БАЗОВИЙ
5.2.5	НХП повинен задокументувати процеси моніторингу викрадених, зламаних облікових даних і блокування ОЗ привілейованих користувачів, що очікує на розгляд уповноваженою особою через виявлену проблему.	СЕРЕДНІЙ
5.2.6	НХП повинен задокументувати процеси моніторингу викрадених, зламаних облікових даних і блокування ОЗ всіх користувачів, які знаходяться під його відповідальністю.	ВИСОКИЙ
5.2.7	НХП повинен автоматично контролювати впроваджені автоматизовані механізми блокування і відкликання ОЗ користувачів, щоб гарантувати їх відповідність.	ВИСОКИЙ

продовження табл. 12

5.ЗУПРАВЛІННЯ ПРАВАМИ ДОСТУПУ		
5.3.1	НХП повинен задокументувати та впровадити процедури надання, оновлення та відкликання прав доступу до ресурсів інформаційної системи хмарного сервісу, які відповідають рольовій концепції та політикам керування правами доступу та своєчасно виконувати ці процедури коли роль та обов'язки працівника змінюються. НХП перевіряє права доступу всіх ОЗ, які знаходяться під його відповідальністю, принаймні раз на рік, щоб переконатись, чи вони відповідають потребам.	БАЗОВИЙ
5.3.2	Оновлення або скасування правд доступу має виконуватись протягом 48 годин для привілейованих користувачів та 14 днів для інших прав доступу.	СЕРЕДНІЙ
5.3.3	НХП повинен запропонувати користувачам самообслуговування, за допомогою якого вони можуть самостійно керувати правами доступу для всіх ОЗ користувачів під їх відповідальність.	СЕРЕДНІЙ
5.3.4	Перевірку прав доступу здійснюють уповноважені особи під відповідальність уповноваженого органу, який затвердив політику доступу. Виявлені відхилення обробляються не пізніше 7 днів після їх знаходження.	СЕРЕДНІЙ
5.3.5	НХП надає користувачам хмарних послуг інструмент, який полегшує перегляд прав доступу ОЗ користувачів, які знаходяться під їхньою відповідальністю. А процедури управління правами доступу повинні дотримуватися динамічного підходу і своєчасно документувати несумісність між правами доступу при їх оновленні.	ВИСОКИЙ

продовження табл. 12

5.3.1	НХП повинен вимагати надійної автентифікації для доступу до інтерфейсів адміністрування, які використовує НХП та користувачі. При цьому права привілейованого доступу повинні бути персоналізовані, обмежені в часі відповідно до оцінки ризику та присвоєні відповідно до необхідності для виконання завдань.	БАЗОВИЙ
5.3.2	Діяльність користувачів з привілейованими правами доступу повинна реєструватись для виявлення зловживань, автоматично відстежуватись на наявність підозрілих подій та повідомляти персонал про потенційні зловживання для вжиття відповідних заходів.	СЕРЕДНІЙ
5.3.3	НХП повинен підтримувати оновлений перелік привілейованих прав доступу і переглядати список привілейованих ОЗ у межах своєї відповідальності кожні три місяці.	ВИСОКИЙ
5.4МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ		
5.4.1	НХП має документувати та впроваджувати політику та процедури щодо надійних механізмів автентифікації, які охоплюють аспекти вибору механізмів, придатних для кожного рівня ризику ОЗ та захист облікових даних.	БАЗОВИЙ
5.4.2	Доступ до всіх середовищ, включаючи невиробничі, а також ті, що містять дані користувачів, повинен мати сильну автентифікацію.	ВИСОКИЙ
5.4.3	Автентифікація користувача повинна виконуватись за допомогою паролів, сертифікатів з цифровим підписом або інших процедур, які досягають еквівалентного рівня безпеки і включати механізм блокування після попередньо визначеної кількості невдалих спроб..	СЕРЕДНІЙ

ДОДАТОК Д

Таблиця 13

Криптографічний захист

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	Спільна	-	+	-	-	-	+	-

№	**Опис вимог**	**Рівень гарантій**
	6.1КРИПТОГРАФІЧНИЙ ЗАХИСТ	
6.1.1	НХП повинен документувати і впроваджувати політики з технічними та організаційними гарантіями для шифрування та керування ключами, включаючи аспекти використання надійних сучасних процедур шифрування, безпечних мережевих протоколів та управління ключами.	БАЗОВИЙ
6.1.2	Політика та процедури криптографії повинні включати положення, засновані на ризиках, щодо використання шифрування, узгодженого зі схемами класифікації даних та з урахуванням каналу зв'язку, типу, сили та якості шифрування.	СЕРЕДНІЙ
6.1.3	НХП визначає і впроваджує надійні механізми шифрування для передачі даних через загальнодоступні мережі.	БАЗОВИЙ

продовження табл. 13

6.2ШИФРУВАННЯ ДАНИХ У СПОКОЇ		
6.2.1	НХП повинен задокументувати та впровадити процедури та технічні засоби захисту для шифрування даних клієнтів хмари під час зберігання.	БАЗОВИЙ
6.2.2	Закриті та секретні ключі, які використовуються для шифрування, повинні бути відомі лише клієнту хмари відповідно до чинних юридичних та нормативних зобов'язань та вимог, з можливістю винятків. Процедури використання закритих і секретних ключів, включаючи процедури винятків, узгоджуються з клієнтом хмари.	СЕРЕДНІЙ
6.2.3	Закриті та секретні ключі, які використовуються для шифрування, повинні бути відомі лише клієнту хмари без винятків відповідно до чинних юридичних та нормативних зобов'язань та вимог.	ВИСОКИЙ
6.3БЕЗПЕЧНЕ УПРАВЛІННЯ КЛЮЧАМИ		
6.3.1	НХП повинен впроваджувати процедури та технічні гарантії для безпечного керування ключами в зоні відповідальності НХП протягом усього життєвого циклу ключів, включаючи генерацію, сертифікацію, активацію, безпечне зберігання, зміну, вилучення і видалення ключів для різних криптографічних систем і додатків.	БАЗОВИЙ
6.3.2	Для безпечного зберігання ключів, система керування ключами має бути відокремлена від прикладного рівня та проміжного ПЗ.	СЕРЕДНІЙ
6.3.3	Для безпечного зберігання ключів та інших секретів, що використовуються для завдань адміністрування, НХП повинен використовувати відповідний захисний контейнер, ПЗ або АЗ.	ВИСОКИЙ

ДОДАТОК Е

Таблиця 14

Операційна безпека

Застосовність та відповідальність			**Архітектурна відповідність**						
IaaS	**PaaS**	**SaaS**	**Обладн.**	**Мережа**	**Обчисл.**	**Пам'ять**	**Додатки**	**Дані**	**Персонал**
Спільна	Спільна	НХП	-	+	-	-	+	+	-

7.1УПРАВЛІННЯ ЗАГРОЗАМИ ТА ВРАЗЛИВОСТЯМИ		
№	**Опис вимог**	**Рівень гарантій**
7.1.1	НХП повинен задокументувати і впроваджувати технічні та організаційні заходи для забезпечення своєчасного виявлення вразливостей, оцінки їх критичності, визначення пріоритетів і усунення у компонентах системи, що використовуються для надання хмарних послуг.	БАЗОВИЙ
7.1.2	НХП має використовувати систему балів для оцінки вразливостей, яка включає принаймні «високий» та «критичний» класи (аналогічні оцінкам 7,0-8,9 та 9,0-10,0 балам CVSS відповідно).	СЕРЕДНІЙ
7.1.3	У своїх політиках і процедурах НХП зобов'язує негайну обробку критичних і високих вразливостей з подальшим спостереженням за їх пом'якшенням.	ВИСОКИЙ

продовження табл. 14

7.1.4	НХП має публікувати та підтримувати загальнодоступний онлайн-реєстр відомих вразливостей, які впливають на хмарні сервіси і активи, опис варіантів їх усунення та інформацію про наявність оновлень для уникнення цих вразливостей.	БАЗОВИЙ
7.1.5	НХП має забезпечити механізми автоматичного оновлення активів, які користувач повинен встановлювати або використовувати під свою власну відповідальність, щоб полегшити розгортання оновлень і виправлення вразливостей системи.	ВИСОКИЙ
7.1.6	НХП повинен регулярно виконувати тести для виявлення загальновідомих вразливостей на системних компонентах, які використовуються для надання хмарних послуг та обробляє кожну ідентифіковану вразливість відповідно до визначених політик і процедур.	СЕРЕДНІЙ
7.1.7	Тестування на проникнення виконуються за багаторічною програмою, враховуючи розвиток хмарного сервісу та поточний ландшафт загроз, а також за допомогою зовнішніх постачальників послуг. За результатами тестувань виконується аналіз першопричин виникнення вразливостей і співвідношення їх до попередніх інцидентів безпеки.	ВИСОКИЙ
7.1.8	НХП повинен регулярно вимірювати, аналізувати та оцінювати процедури і засоби за допомогою яких обробляються вразливі місця та інциденти, щоб перевірити їх придатність, доречність та ефективність.	БАЗОВИЙ

продовження табл. 14

7.2ЛОГУВАННЯ ТА МОНІТОРИНГ		
7.2.1	НХП повинен документувати та впроваджувати політику та процедури, які керують логуванням та моніторингом подій на компонентах системи, що передбачають визначення подій, які можуть привести до порушення безпеки, специфікації для активації і зупинки ведення журналів, інформацію щодо термінів зберігання журналів, процедури їх захисту й видалення, ролі та відповідальність за налаштування, конфігурацію та моніторинг журналу подій, а також часову синхронізацію компонентів системи.	БАЗОВИЙ
7.2.2	НХП повинен відстежувати дані журналу, щоб ідентифікувати події, які можуть привести до інцидентів безпеки відповідно до вимог реєстрації й моніторингу та повідомляти про виявлені інциденти безпеки відповідні підрозділи для своєчасної оцінки та усунення..	БАЗОВИЙ
7.2.3	Моніторинг подій має бути автоматизованим, а зв’язок між активами, які підлягають логуванню і серверами реєстрації має бути зашифровано з використанням сучасних криптографічних засобів або має відбуватись у віддаленій мережі адміністрування.	СЕРЕДНІЙ

продовження табл. 14

7.ЗРЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ		
7.3.1	НХП повинен документувати та впроваджувати політику та процедури, що містять технічні та організаційна засоби захисту для забезпечення швидкого, ефективного реагування на всі відомі інциденти безпеки, які включають вказівки щодо класифікації, визначення пріоритетів, аналізу першопричин подій та ескалації інцидентів безпеки, створюють інтерфейси управління інцидентами та управління безперервністю бізнесу.	БАЗОВИЙ
7.3.2	НХП створює групу реагування на інциденти, яка сприяє скоординованому розслідуванню інцидентів з безпеки.	БАЗОВИЙ
7.3.3	НХП повинен документувати заходи після обробки інциденту безпеки та своєчасно інформувати клієнтів, які постраждали від інцидентів безпеки за визначеною процедурою.	СЕРЕДНІЙ
7.3.4	Політика управління інцидентами повинна включати методологію оцінки, щоб зібрана інформація в подальшому не втратила свою доказову цінність.	ВИСОКИЙ
7.3.5	Політика управління інцидентами включає положення щодо регулярного тестування можливостей реагування на інциденти для визначення ефективності системи, виявлення потенційних недоліків та вдосконалення плану реагування на інциденти безпеки.	ВИСОКИЙ

ДОДАТОК Є
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в іноземних виданнях

1. Anna Torchylo, Andrii Bigdan, Tetiana Babenko. "Analysis of "Fileless" Malware and Attacks", II International Conference “Engineer of XXI Century”, Bielsko-Biala, Poland. – 2020.

Статті у наукових фахових виданнях України

1. Yanina Shestak, Sergii Tolupa, Anna Torchylo, Ogbu James Onyigwang. Analysis of Methods for Data Structuring in Data Centers. 2021 IEEE International Conference on Problems of Infocommunications. Science and Technology, PICST 2021, - p. 76 (Scopus).

Тези наукових доповідей:

1. Шестак Я.В., Толюпа С.В., Торчило А.П., Мирутенко Л. В. Аналіз ефективності застосування сучасних технологій структурування даних у центрах їх обробки. Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції, ПНЗІ 2021, Одеса-Тернопіль – 8 с.
2. Шестак Я., Панасюк О., Торчило А., Огбу Д. Метод кластеризацій, як головний напрямок забезпечення захисту ЦОД. 13-а Всеукраїнська науково-практична конференція Стан та удосконалення безпеки інформаційно–телекомунікаційних систем, SITS 2021, Миколаїв – Коблево – 7 с.
3. Yanina Shestak, Sergii Tolupa, Anna Torchylo. Network System Structure Design for Data Centers. The 1st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things, TTSIIT 2022, Ukraine-Iraq-Poland – p. 23.
4. Anna Torchylo, Andrii Bigdan, Tetiana Babenko. Preventing and Detecting Cryptocurrency Mining Malware. Cyber Security Problems of Information and Telecommunication Systems, PCSITS 2021, - p. 77.